

Martha Rzedowski Calderón

Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.
mrzedowski@ctrl.cinvestav.mx

Gabriel Villa Salvador

Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.
gvilla@ctrl.cinvestav.mx

Campos ciclotómicos

Numéricos y de funciones (versión preliminar)

11 de julio de 2014



Departamento de Control Automático

Centro de Investigación y de Estudios Avanzados del
I.P.N.

México D. F.

A Sofía y a mis padres

A Sofía y a la memoria de mis padres

A los que se doblan pero no se doblegan

*Si nunca se pide un imposible a un alumno, nunca enseñará de lo
que es capaz.*

*El arte de la enseñanza es dar la impresión de haber sabido toda la
vida lo que aprendimos en la noche anterior.*

****.

Introducción

Los campos ciclotómicos tuvieron su origen en el trabajo de Kummer en 1847 sobre el Último Teorema de Fermat. Un campo ciclotómico $\mathbb{Q}(\zeta_n)$ es simplemente agregar al campo de los números racionales \mathbb{Q} las raíces de la ecuación $x^n - 1$ donde n es un número natural.

Una de las razones para escribir este libro, se debe a la ausencia de un trabajo más o menos exhaustivo sobre los campos ciclotómicos en español. Tenemos que el tema de los campos ciclotómicos es tratado en todos los libros introductorios de Teoría de Números, así como en libros sobre campos numéricos y en los tratados generales de Álgebra, sin embargo, casi todos estos libros han sido escritos ya sea en inglés, francés, ruso o alemán y pocos de ellos han sido traducidos a nuestro idioma. Por otro lado hay relativamente pocos libros sobre el tema escritos originalmente en español.

Debemos hacer notar que este trabajo toca únicamente la superficie de la teoría de campos ciclotómicos y no trata sobre muchos de los temas presentados en libros como los de L. Washington [75] o el de S. Lang [43]. Por otro lado hemos incluido el tema de los campos de funciones ciclotómicas que muestra nuevamente y de manera clara la similitud que existe entre los campos numéricos y los campos de funciones.

La importancia de los campos ciclotómicos es su simplicidad y su utilidad y relevancia para diversos objetivos, como son el estudio de las extensiones abelianas, su uso para el estudio del Último Teorema de Fermat, ejemplifican de diversas formas conceptos que usualmente son de difícil acceso como son la ramificación, los discriminantes, las bases enteras y así sucesivamente.

Suponemos que el lector está familiarizado con un curso general de Teoría de Números y uno sobre Teoría de Galois y que conoce, aunque sea de manera superficial, los conceptos de dominios de Dedekind, anillos de enteros, discriminante, diferente, bases enteras, etc.

Mucho de lo que presentamos en este libro está basado en el libro de Washington mencionado anteriormente. Nuestro primer capítulo es una compilación de varios conceptos y resultados que usaremos a lo largo de este tra-

VIII

bajo: discriminante, diferente, grupos de descomposición e inercia, así como los grupos de ramificación para el estudio de la ramificación salvaje.

El Capítulo 2 presenta la Teoría de Galois de extensiones infinitas con el objetivo de estudiar la Teoría de Iwasawa la cual veremos en el Capítulo 13. El Capítulo 3 es la introducción a los campos ciclotómicos. En el Capítulo 4 damos una demostración del teorema clásico de Kronecker–Weber basada en la demostración dada por D. Hilbert [27] usando los grupos de ramificación.

El Capítulo 5 trata sobre un caso especial del Teorema de Dirichlet sobre la infinidad de números primos en progresiones aritméticas y el estudio de los subcampos de los campos ciclotómicos $\mathbb{Q}(\zeta_{p^m})$ donde p es un número primo.

En el Capítulo 6 usamos los caracteres de Dirichlet para el estudio aritmético de las extensiones abelianas de \mathbb{Q} , tal como fue introducido por Leopoldt [46]. En el Capítulo 7 probamos el caso general del Teorema de Dirichlet antes mencionado.

El Capítulo 8 da una breve introducción a los campos de funciones y el Capítulo 9 desarrolla los campos de funciones ciclotómicos basados en los trabajos de Carlitz [9, 10] y de Hayes [25] los cuales son análogos a los campos ciclotómicos numéricos. En el Capítulo 10 presentamos una teoría de extensiones de campos de funciones con campo de constantes un campo finito, los cuales están generados por elementos de torsión bajo la acción de Carlitz–Hayes. Esta teoría puede ser considerada como una teoría de tipo de Kummer para extensiones del tipo de Carlitz–Hayes.

En el Capítulo 11 damos una breve introducción a los vectores de Witt los cuales estudian los p -extensiones cíclicas en característica p . También damos las diversas definiciones de conductor y establecemos algunas de sus relaciones. En el Capítulo 12 damos dos aplicaciones de lo desarrollado anteriormente: una demostración combinatoria del análogo del Teorema de Kronecker–Weber para campos de funciones racionales congruentes y los campos de géneros de campos de funciones.

El último capítulo trata sobre la Teoría de Iwasawa. En esta última parte, nos basamos en los Capítulos 7 y 13 de [75]. Para poder dar una introducción a la Teoría de Iwasawa hemos necesitado usar varios teoremas de Teoría de Campos de Clases los cuales escapan a los alcances de este escrito y por tanto los hemos usado sin demostración en varios casos. El lector puede, sin perder continuidad, esquivar las partes técnicas de estos teoremas.

Martha Rzedowski Calderón,
Gabriel D. Villa Salvador.
México, D.F., 11 de julio de 2014.

Índice general

1. Teoría algebraica de números	1
1.1. Discriminante y diferente	1
1.2. Ramificación en campos numéricos	4
1.3. Grupos de inercia, de descomposición y de ramificación	6
1.4. Primos infinitos	12
2. Teoría de Galois infinita	15
2.1. Límites directos y límites inversos	15
2.2. Teoría de Galois infinita	22
3. Campos ciclotómicos	25
3.1. La función exponencial y el número π	25
3.2. Campos Ciclotómicos	28
3.2.1. Estructura de U_n	35
4. Teorema de Kronecker–Weber	51
4.1. El teorema y su demostración	51
4.2. Caso central: ramificación salvaje	54
5. Propiedades y aplicaciones de los campos ciclotómicos	61
5.1. Caso especial del Teorema de Dirichlet	61
5.2. Descomposición de primos en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$	63
5.3. Subcampos de $\mathbb{Q}(\zeta_n)$	72
5.3.1. Subcampos de $\mathbb{Q}(\zeta_{2^m})$	73
5.3.2. Subcampos de $\mathbb{Q}(\zeta_{p^m})$, p primo, $p > 2$	75
5.3.3. Subcampos cuadráticos	77
5.4. Anillos de enteros y unidades	79
5.5. Teorema de reciprocidad cuadrática	80

6. Caracteres de Dirichlet	83
6.1. Teoría de caracteres	83
6.2. Caracteres de Dirichlet	88
6.3. Aritmética de $\mathbb{Q}(\zeta_n)$ usando caracteres	103
6.3.1. Fórmula del Conductor–Discriminante	107
6.4. Construcción de extensiones abelianas	112
6.4.1. Campos de géneros	112
6.4.2. Grupos abelianos como grupos de Galois y de clases	121
7. Series L de Dirichlet	125
7.1. Teorema de Dirichlet	125
8. Campos de funciones	139
8.1. Generalidades	139
8.2. Valuaciones en $k(x)$	140
8.3. Reparticiones y diferenciales	142
8.4. Extensiones de Galois	145
8.5. Diferente, discriminante y ramificación	146
8.6. Formula de Riemann–Hurwitz	148
9. Campos de funciones ciclotómicos	151
9.1. Campos de funciones congruentes	151
9.2. Campos ciclotómicos	153
9.3. Ramificación en $K(A_M)/K$	165
9.4. Caracteres de Dirichlet	171
9.5. Caracteres de Dirichlet y aritmética de campos de funciones ciclotómicos	182
9.6. Fórmula del conductor–discriminante	189
10. Extensiones radicales de campos de funciones	199
10.1. Introducción	199
10.2. Extensiones de Kummer de campos de funciones	201
10.2.1. Algo sobre la teoría de módulos	202
10.3. Teoría de Kummer	205
10.4. Extensiones radicales ciclotómicas	208
10.5. Algunas propiedades de las extensiones radicales	211
10.6. Algunas propiedades de las extensiones radicales ciclotómicas	213
10.7. Algunos teoremas de estructura de extensiones radicales ciclotómicas	216
10.8. Ejemplos y aplicaciones	219
10.9. Una cota para $ \text{cog}(L/\mathcal{K}) $	229

11. Extensiones p-cíclicas en característica p	237
11.1. Introducción	237
11.2. Extensiones de Artin–Schreier	238
11.3. La construcción de Schmid	241
11.4. Vectores de Witt	243
11.5. Aritmética de los vectores de Witt	248
11.6. Vectores de Witt en característica p	249
11.7. Extensiones cíclicas de grado p^n en característica p	253
11.8. Sobre el conductor	258
11.8.1. Representaciones, caracteres y conductores	261
11.8.2. Conductores de Artin	262
11.8.3. Conductor local de $K(\Lambda_{P^\alpha})$	264
11.8.4. El conductor de acuerdo a Schmid	265
12. El teorema de Kronecker–Weber en característica p y campos de géneros	269
12.1. Introducción	269
12.2. El Teorema de Kronecker–Weber para campos de funciones	270
12.2.1. Extensiones geométricas moderadamente ramificadas	271
12.2.2. Extensiones salvajemente ramificadas	274
12.3. Campo de géneros	289
12.3.1. Campos de funciones congruentes generales	292
12.3.2. Aplicaciones	298
13. Teoría de Iwasawa	303
13.1. Campos ciclotómicos infinitos	303
13.2. Ramificación en extensiones algebraicas	304
13.3. Pro- p -grupos	309
13.4. Extensiones \mathbb{Z}_p	310
13.5. Ramificación y descomposición de primos en $\mathbb{Q}_\infty/\mathbb{Q}$	314
13.6. Estructura de $\Lambda = \mathbb{Z}_p[[T]]$ -módulos	326
13.7. Los invariantes de Iwasawa	337
13.8. Ejemplo de $\mu > 0$	370
Referencias	377

Teoría algebraica de números

En este capítulo introductorio, pretendemos recordar rápidamente varios conceptos que, en diversa medida, nos servirán para nuestros objetivos en este libro. Todos los resultados pueden ser consultados en [27, 38, 42, 48, 49, 67].

1.1. Discriminante y diferente

Por un campo numérico K entenderemos una extensión del campo de los números racionales \mathbb{Q} y \mathcal{O}_K denota el anillo de los enteros de K , es decir, $\mathcal{O}_K := \{\alpha \in K \mid \text{Irr}(\alpha, x, \mathbb{Q}) \in \mathbb{Z}[x]\}$, donde $\text{Irr}(\beta, t, E)$ denota al polinomio mónico de mínimo grado $f(t)$ en la variable t sobre el campo E , $f(t) \in E[t]$, tal que $f(\beta) = 0$.

Resulta ser que \mathcal{O}_K es un \mathbb{Z} -módulo libre de rango $[K : \mathbb{Q}]$. En general, si L/K es una extensión de campos numéricos, \mathcal{O}_L no necesariamente es un \mathcal{O}_K -módulo libre. Lo que sí se tiene es que

$$\mathcal{O}_L \cong \mathcal{O}_K^{[L:K]-1} \oplus I$$

como \mathcal{O}_K -módulos, donde I es un ideal de \mathcal{O}_K .

Empezamos con el resultado de Dirichlet sobre las unidades.

Teorema 1.1.1 (Teorema de las unidades de Dirichlet). *Sea K cualquier campo numérico, $[K : \mathbb{Q}] = r_1 + 2r_2 = n < \infty$, donde r_1 es el número de encajes reales de K y $2r_2$ es el número de encajes complejos de K . Sea U_K el grupo de unidades de K , es decir del anillo de enteros \mathcal{O}_K de K : $U_K = \mathcal{O}_K^*$. Entonces, como grupos, tenemos $U_K \cong W_K \times \mathbb{Z}^{r_1+r_2-1}$ donde W_K son las raíces de unidad que hay en \mathcal{O}_K . En otras palabras, existen unidades $w_1, \dots, w_{r_1}, w_{r_1+1}, \dots, w_{r_1+r_2-1}$ tales que todo elemento u de U_K se escribe de manera única como*

$$u = \zeta w_1^{\alpha_1} \cdots w_{r_1+r_2-1}^{\alpha_{r_1+r_2-1}}$$

con ζ una raíz de unidad en K y $\alpha_1, \dots, \alpha_{r_1+r_2+1} \in \mathbb{Z}$. En particular, el grupo de torsión de U_K es W_K . \square

Sea L/K una extensión de campo numéricos.

Para cualquier sistema $\{\xi_1, \dots, \xi_n\} \subseteq \mathcal{O}_L$ se define el *discriminante* de $\{\xi_1, \dots, \xi_n\}$ por

$$\mathfrak{d}_{L/K}(\xi_1, \dots, \xi_n) = \left(\det[\sigma_j \xi_i]_{1 \leq i, j \leq n} \right)^2 = \det(\mathrm{Tr}_{L/K} \xi_i \xi_j)$$

donde $\sigma_1, \dots, \sigma_n$ son los $n = [L : K]$ diferentes K -encajes de L en una cerradura algebraica \bar{K} de K y $\mathrm{Tr}_{L/K}$ denota la traza de L a K .

Si $L = K(a)$ y $p(x) = \mathrm{Irr}(a, x, K)$ entonces

$$\begin{aligned} \mathfrak{d}_{L/K}(a) &:= \mathfrak{d}_{L/K}(1, a, a^2, \dots, a^{n-1}) = \prod_{i < j} (\sigma_i(a) - \sigma_j(a))^2 \\ &= (-1)^{n(n-1)/2} N_{L/K}(p'(a)) \end{aligned}$$

donde $N_{L/K}(a)$ denota la norma de a .

Sea $\{\alpha_1, \dots, \alpha_n\}$ una base entera de K/\mathbb{Q} , es decir, $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$, y $\{\beta_1, \dots, \beta_n\} \subset \mathcal{O}_K$. Entonces si $\beta_i = \sum_{j=1}^n a_{ij} \alpha_j$, $n = [K : \mathbb{Q}]$ con $a_{ij} \in \mathbb{Z}$, se tiene

$$\mathfrak{d}_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n) = m^2 \mathfrak{d}_{L/K}(\alpha_1, \dots, \alpha_n), \quad m = \det[a_{ij}] \in \mathbb{Z}$$

y en particular, si $\{\beta_1, \dots, \beta_n\}$ es también una base entera, entonces $m = \pm 1$ y

$$\delta_K := \mathfrak{d}_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n) = \mathfrak{d}_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$$

se llama el *discriminante del campo* y es independiente de la base entera.

Se tiene que el signo de δ_K es igual a $(-1)^{r_2}$ donde $[K : \mathbb{Q}] = r_1 + 2r_2$, r_1 es el número de encajes reales de K y $2r_2$ es el número de encajes complejos, esto es, no reales, de K . Para una demostración ver Teorema 3.2.23. Además se tiene que

$$\delta_K \equiv 0 \text{ ó } 1 \text{ mód } 4.$$

Para una extensión L/K cualquiera de campos numéricos, sea $M \subseteq L$ un subgrupo aditivo de L . El *módulo complementario* a M se define por:

$$M' := \{x \in L \mid \mathrm{Tr}_{L/K}(xm) \in \mathcal{O}_K \ \forall m \in M\}.$$

Notemos que si M es un \mathcal{O}_K -módulo, entonces M' también es un \mathcal{O}_K -módulo. Ahora bien, si $\{\alpha_1, \dots, \alpha_n\}$ es una base de L/K , la *base dual* de $\{\alpha_1, \dots, \alpha_n\}$ se define por $\{\alpha'_1, \dots, \alpha'_n\}$ donde

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha'_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}, \quad 1 \leq i, j \leq n.$$

Si $M = \mathcal{O}_K \alpha_1 + \dots + \mathcal{O}_K \alpha_n$, entonces se tiene que $M' = \mathcal{O}_K \alpha'_1 + \dots + \mathcal{O}_K \alpha'_n$.

El *diferente* $\mathfrak{D}_{L/K}$ de L/K se define por

$$\mathfrak{D}_{L/K}^{-1} := \mathcal{O}'_L$$

es decir, como el inverso del módulo complementario de \mathcal{O}_L .

Si \mathcal{P} es un ideal primo de \mathcal{O}_K , se define la *conorma* de \mathcal{P} por

$$\text{con}_{K/L} \mathfrak{p} = \mathfrak{p} \mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Si $K \subseteq L \subseteq F$ es una torre de campos numéricos, entonces se tiene que

$$\mathfrak{D}_{F/K} = \mathfrak{D}_{F/L} \text{con}_{L/F} \mathfrak{D}_{L/K}.$$

El *discriminante* $\mathfrak{d}_{L/K}$ de la extensión L/K se define por

$$\mathfrak{d}_{L/K} := N_{L/K} \mathfrak{D}_{L/K}.$$

Se tiene que $\mathfrak{d}_{L/\mathbb{Q}} = \langle \delta_L \rangle$.

Un resultado muy útil para el cálculo del diferente, es el siguiente:

Teorema 1.1.2. *Se tiene que $\mathfrak{D}_{L/K}$ es el máximo común divisor del conjunto*

$$\begin{aligned} & \{f'(\alpha) \mid \alpha \in \mathcal{O}_L, L = K(\alpha), f(x) = \text{Irr}(\alpha, x, K)\} \\ &= \langle f'(\alpha) \mid \alpha \in \mathcal{O}_L, L = K(\alpha), f(x) = \text{Irr}(\alpha, x, K) \rangle. \end{aligned} \quad \square$$

Corolario 1.1.3. *Si $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ entonces $\mathfrak{D}_{L/K} = \langle f'(\alpha) \rangle$ donde $f(x) := \text{Irr}(\alpha, x, K)$.* \square

Es decir, en general tenemos para una extensión L/K :

$$\mathfrak{D}_{L/K} = \langle f'(\alpha) \mid \alpha \in \mathcal{O}_L, L = K(\alpha), f(x) = \text{Irr}(\alpha, x, K) \rangle$$

y

$$\mathfrak{d}_{L/K} = \langle N_{L/K} f'(\alpha) \mid \alpha \in \mathcal{O}_L, L = K(\alpha), f(x) = \text{Irr}(\alpha, x, K) \rangle.$$

En particular, si $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\mathfrak{D}_{L/\mathbb{Q}} = \langle f'(\alpha) \rangle$ y

$$\delta_K = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\alpha)) = \prod_{i < j} (\alpha^{(i)} - \alpha^{(j)})^2$$

donde $\alpha = \alpha^{(1)}, \dots, \alpha^{(n)}$ son los conjugados de α y $n = [K : \mathbb{Q}]$.

Teorema 1.1.4 (Kummer). *Sean A un dominio Dedekind, $K = \text{coc } A$ el campo de cocientes de A . Sean E/K una extensión finita y separable y B la cerradura entera de A en E . Supongamos que existe $\alpha \in B$ tal que $B = A[\alpha]$. Sea $f(x) := \text{Irr}(\alpha, x, \mathbb{Q})$. Fijemos un primo \mathfrak{p} en A . Sea $\overline{f(x)} := f(x) \bmod \mathfrak{p}$ y*

sea $\overline{f(x)} = \overline{P_1(x)}^{e_1} \cdots \overline{P_g(x)}^{e_g}$ la factorización de $\overline{f(x)}$ en factores irreducibles mónicos en $(A/\mathfrak{p})[x]$ y $P_i(x) \in A[x]$ mónico. Entonces

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \quad \begin{array}{ccccc} \mathfrak{P}_1, \dots, \mathfrak{P}_g & \text{---} & B & \text{---} & E \\ | & & | & & | \\ \mathfrak{p} & \text{---} & A & \text{---} & K \end{array}$$

donde $\mathfrak{P}_i = \mathfrak{p} + \langle P_i(\alpha) \rangle$, es su descomposición como producto de ideales primos de B . \square

Theorem 1.1.5 (Dedekind). Sea L/K una extensión de campos numéricos y \mathcal{P} un ideal primo no cero de \mathcal{O}_K . Entonces si

$$\text{con}_{L/K} \mathcal{P} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

se tiene que algún $e_i > 1$, es decir, \mathfrak{p}_i es ramificado y \mathcal{P} es ramificado si y solamente si $\mathfrak{p}_i | \mathfrak{D}_{L/K}$ y $\mathcal{P} | \mathfrak{D}_{L/K}$.

Demostración. Presentamos un esquema de una parte de la demostración para K/\mathbb{Q} .

Si $p \in \mathbb{Z}$ es un número primo, $\mathfrak{p} \subseteq \mathcal{O}_K$ es un primo encima de p y $\mathfrak{D}_{K/\mathbb{Q}}$ es el diferente de K/\mathbb{Q} , entonces veremos que si $\mathfrak{p}^e | \langle p \rangle$, se tiene que $\mathfrak{p}^{e-1} | \mathfrak{D}_{K/\mathbb{Q}}$ lo cual implicará en particular que si \mathfrak{p} es ramificado, entonces $e \geq 2$ y por lo tanto $e - 1 \geq 1$ y en particular $\mathfrak{p} | \mathfrak{D}$.

Para probar la afirmación anterior pongamos $(p) = p\mathcal{O}_K = \mathfrak{p}^m \mathfrak{a}$ con $(\mathfrak{a}, \mathfrak{p}) = 1$ y $m \geq e$. Entonces si $x \in \mathfrak{p}\mathfrak{a}$, $x = \sum_{i=1}^n \alpha_i \beta_i$ con $\alpha_i \in \mathfrak{p}, \beta_i \in \mathfrak{a}$. Por tanto $x^{p^t} \equiv \sum_{i=1}^n \alpha_i^{p^t} \beta_i^{p^t} \pmod{p}$. Para t suficientemente grande se tiene que $\alpha_i^{p^t} \in \mathfrak{p}^m$ y por tanto $x^{p^t} \in \mathfrak{p}^m \mathfrak{a} = \langle p \rangle$. En particular obtenemos que $\text{Tr}_{K/\mathbb{Q}} x^{p^t} \in p\mathbb{Z}$.

Se tiene que $\text{Tr}_{K/\mathbb{Q}} x^{p^t} \in p\mathbb{Z} \Rightarrow (\text{Tr}_{K/\mathbb{Q}} x)^{p^t} \in p\mathbb{Z} \Rightarrow \text{Tr}_{K/\mathbb{Q}} x \in p\mathbb{Z} \Rightarrow \text{Tr}_{K/\mathbb{Q}}(p^{-1}\mathfrak{p}\mathfrak{a}) \subseteq \mathbb{Z} \Rightarrow p^{-1}\mathfrak{p}\mathfrak{a} \subseteq \mathfrak{D}_{K/\mathbb{Q}}^{-1} \Rightarrow \mathfrak{D}_{K/\mathbb{Q}} p^{-1}\mathfrak{p}\mathfrak{a} \subseteq \mathcal{O}_K \Rightarrow \mathfrak{D}_{K/\mathbb{Q}} \subseteq p\mathfrak{p}^{-1}\mathfrak{a}^{-1} = \mathfrak{p}^m \mathfrak{a} \mathfrak{p}^{-1} \mathfrak{a}^{-1} = \mathfrak{p}^{m-1} \Rightarrow \mathfrak{p}^{m-1} | \mathfrak{D}_{K/\mathbb{Q}}$. \square

1.2. Ramificación en campos numéricos

Los resultados que aquí presentamos pueden ser consultados en [42] y en [49, Capítulo 4].

Uno de los problemas centrales que se presentan en la Teoría de Números es el problema de la *ramificación*. Recordaremos a continuación algunos resultados generales que aplicaremos a nuestro caso particular de los campos ciclotómicos.

Como hemos recordado anteriormente, el diferente inverso $\mathfrak{D}_{L/K}^{-1}$ de una extensión de campos numéricos está dado como el módulo complementario del anillo de enteros \mathcal{O}_L mediante la traza. Más precisamente

$$\mathfrak{D}_{L/K}^{-1} := \{x \in L \mid \text{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\} =: \mathcal{O}'_L. \quad (1.1)$$

Se tiene que $\mathfrak{D}_{L/K}^{-1} \supseteq \mathcal{O}_L$ y es un ideal fraccionario.

Si \mathcal{P} es un ideal primo no cero de \mathcal{O}_K , entonces el ideal extendido en \mathcal{O}_L : $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde

$$[L : K] = \sum_{i=1}^g e_i f_i \quad \text{y} \quad f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

Si $e_i > 1$ decimos que \mathfrak{P}_i es *ramificado* y que \mathfrak{p} es *ramificado*. Además tenemos que $N_{L/K}\mathfrak{P}_i = \mathfrak{p}^{f_i}$.

La conexión entre el diferente y la ramificación está explícitamente dada en el siguiente resultado, el cual precisa el Teorema 1.1.5.

Teorema 1.2.1. *Si \mathfrak{p} es un ideal no primo de \mathcal{O}_K y si $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, entonces $\mathfrak{P}_i^{e_i-1} \mid \mathfrak{D}_{L/K}$. Más aún, $\mathfrak{P}_i^{e_i} \mid \mathfrak{D}_{L/K}$ si y solamente si $p \mid e_i$ donde p es la característica del campo residual $\mathcal{O}_K/\mathfrak{p}$.* \square

Corolario 1.2.2. *Se tiene que $\mathfrak{P} \mid \mathfrak{D}_{L/K}$ si y solamente si \mathfrak{P} es ramificado.* \square

Corolario 1.2.3. *El número de primos de \mathcal{O}_L ramificados en L/K es finito y los primos ramificados son exactamente los divisores de $\mathfrak{D}_{L/K}$.* \square

Definición 1.2.4. Con las notaciones anteriores, decimos que \mathfrak{p} (o que \mathfrak{P}_i) es *salvajeamente ramificado* si $p \mid e_i$ y *moderadamente ramificado* si $p \nmid e_i$.

Con respecto al discriminante, tenemos:

Corolario 1.2.5. *El número de primos de \mathcal{O}_K ramificados en L es finito y los primos ramificados son exactamente los divisores de $\mathfrak{d}_{L/K}$.* \square

Notación 1.2.6. Cuando $K = \mathbb{Q}$, ponemos simplemente $\mathfrak{d}_L := \mathfrak{d}_{L/\mathbb{Q}}$ y $\mathfrak{D}_L := \mathfrak{D}_{L/\mathbb{Q}}$.

Ejemplo 1.2.7. Consideremos una extensión cuadrática de \mathbb{Q} : $L := \mathbb{Q}(\sqrt{d})$ donde $d \in \mathbb{Z}$ es libre de cuadrados, esto es, $d = p_1 \cdots p_r$ donde p_1, \dots, p_r son primos distintos.

Se tiene que $\sqrt{d} \in \mathcal{O}_L$ y que $f(x) = \text{Irr}(\sqrt{d}, x, \mathbb{Q}) = x^2 - d$. Por tanto $f'(\sqrt{d}) = 2\sqrt{d}$. Se sigue que $\mathfrak{D}_L \mid \langle 2\sqrt{d} \rangle$ y que $\mathfrak{d}_L \mid \langle N_{L/\mathbb{Q}}(2\sqrt{d}) \rangle = \langle -4d \rangle = \langle 4d \rangle$. En particular, los primos ramificados se encuentran en $\{2, p_1, \dots, p_r\}$.

Sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_L$. Si $b = 0$, entonces $\alpha = a \in \mathbb{Z}$ e $\text{Irr}(\alpha, x, \mathbb{Q}) = x - \alpha =: p_\alpha(x)$. Se tiene $p'_\alpha(x) = 1$. Si $b \neq 0$, entonces $\text{Irr}(\alpha, x, \mathbb{Q}) = (x - a)^2 -$

$b^2d = p_\alpha(x) = x^2 - 2ax + a^2 - b^2d \in \mathbb{Z}[x]$. Obtenemos que $p'_\alpha(\alpha) = 2(\alpha - a) = 2b\sqrt{d}$ y $N_{L/\mathbb{Q}}(p'_\alpha(\alpha)) = -4b^2d = (2b)^2(-d) \in \mathbb{Z}$.

Puesto que $b \in \mathbb{Q}$ y $(2b)^2d \in \mathbb{Z}$, si escribimos $b = \frac{\gamma}{\beta}$ con $\gamma, \beta \in \mathbb{Z}$ y primos relativos se tiene que $\beta|2$ pues si algún número primo p divide a β , entonces tenemos que $(2b)^2 = \frac{4\gamma^2}{p^2\beta_1}$ lo cual implica que $p^2|4$. En particular obtenemos que

$$\langle N_{L/\mathbb{Q}}(p'_\alpha(\alpha)) \mid \alpha \in \mathbb{Q} \rangle = \begin{cases} \langle d \rangle & \text{si existe } \alpha = a + b\sqrt{d} \in \mathcal{O}_L, b \notin \mathbb{Z} \\ \langle 4d \rangle & \text{en otro caso.} \end{cases}$$

Ahora si existe $\alpha = a + b\sqrt{d} \in \mathcal{O}_L$ con $b \notin \mathbb{Z}$, entonces $b = \frac{b_1}{2}$ con $b_1 \in \mathbb{Z}$ impar. Tenemos que si $a \in \mathbb{Z}$, entonces $b\sqrt{d} \in \mathcal{O}_L$ pero $\text{Irr}(b\sqrt{d}, x, \mathbb{Q}) = x^2 - b^2d \notin \mathbb{Z}[x]$ lo cual es absurdo. Se sigue que $a \notin \mathbb{Z}$ pero $2a \in \mathbb{Z}$, esto es, $a = \frac{a_1}{2}$ con a_1 impar.

Obtenemos que $a^2 - b^2d = \frac{a_1^2}{4} - \frac{b_1^2}{4}d = \frac{a_1^2 - b_1^2d}{4} \in \mathbb{Z}$ lo cual implica que $a_1^2 - b_1^2d \equiv 0 \pmod{4}$. Por lo tanto $1 \equiv a_1^2 \equiv b_1^2d \pmod{4} \equiv d \pmod{4}$. De esto se obtiene que $d \equiv 1 \pmod{4}$ y $\mathfrak{d}_{\mathbb{Q}(\sqrt{d})} = \langle d \rangle$.

En otro caso, esto es, si $d \not\equiv 1 \pmod{4}$, entonces $d \equiv 2, 3 \pmod{4}$ y $\mathfrak{d}_{\mathbb{Q}(\sqrt{d})} = \langle 4d \rangle$. Escribiendo $p_i \mathcal{O}_L \mathbb{Q}(\sqrt{d}) = \mathfrak{P}_i^2$, $1 \leq i \leq r$, se obtiene finalmente,

$$\mathfrak{d}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathfrak{P}_1 \cdots \mathfrak{P}_r, & d \equiv 1 \pmod{4}, \\ \mathfrak{P}_0^2 \mathfrak{P}_1 \cdots \mathfrak{P}_r, & d \equiv 3 \pmod{4}, \\ \mathfrak{P}_1^3 \mathfrak{P}_2 \cdots \mathfrak{P}_r, & d \equiv 2 \pmod{4}, \quad p_1 = 2, \end{cases}$$

donde $2\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{P}_0^2$ cuando $d \equiv 3 \pmod{4}$.

1.3. Grupos de inercia, de descomposición y de ramificación

Para estudiar ramificación en extensiones de Galois tenemos a nuestra disposición los grupos de inercia, de descomposición y de ramificación. Más precisamente, sea L/K una extensión de Galois de campos numéricos. Sea \mathfrak{p} un primo en \mathcal{O}_K y sea \mathfrak{P} un primo en \mathcal{O}_L que divide a \mathfrak{p} , esto es, $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}\mathfrak{a}$ con \mathfrak{a} un ideal de \mathcal{O}_L . Sea $G := \text{Gal}(L/K)$. Se define:

Definición 1.3.1. El grupo de descomposición $D(\mathfrak{P}|\mathfrak{p})$ se define por

$$D(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Notemos que si $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ entonces $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ y por tanto σ induce un automorfismo

$$\tilde{\sigma}: \mathcal{O}_L/\mathfrak{P} \rightarrow \mathcal{O}_L/\mathfrak{P}$$

tal que $\tilde{\sigma}|_{\mathcal{O}_K/\mathfrak{p}} = \text{Id}_{\mathcal{O}_K/\mathfrak{p}}$. En otras palabras $\tilde{\sigma} \in \text{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. El mapeo

$$\begin{aligned}\theta: G &\rightarrow \text{Gal}(\mathcal{O}_L/\mathcal{O}_K) \\ \sigma &\mapsto \tilde{\sigma}\end{aligned}$$

es un epimorfismo. El núcleo de θ es el *grupo de inercia* de \mathfrak{P} sobre \mathfrak{p} . Más precisamente

Definición 1.3.2. El *grupo de inercia* $I(\mathfrak{P}|\mathfrak{p})$ de \mathfrak{P} sobre \mathfrak{p} se define por

$$I(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid \tilde{\sigma} = \text{Id}_{\mathcal{O}_L/\mathfrak{P}}\} = \{\sigma \in G \mid \sigma x - x \in \mathfrak{P} \ \forall x \in \mathcal{O}_L\}.$$

Se tiene que

$$\frac{D(\mathfrak{P}|\mathfrak{p})}{I(\mathfrak{P}|\mathfrak{p})} \cong \text{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}).$$

En particular tenemos que el *grado relativo* es

$$f(\mathfrak{P}|\mathfrak{p}) := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = \frac{|D(\mathfrak{P}|\mathfrak{p})|}{|I(\mathfrak{P}|\mathfrak{p})|}.$$

Más aún, el *índice de ramificación* $e(\mathfrak{P}|\mathfrak{p}) = e$ de \mathfrak{P} sobre \mathfrak{p} , es decir $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e \mathfrak{a}$ con \mathfrak{a} de \mathcal{O}_L y \mathfrak{P} y \mathfrak{a} primos relativos, es igual a la cardinalidad de $I(\mathfrak{P}|\mathfrak{p})$:

$$e(\mathfrak{P}|\mathfrak{p}) = |I(\mathfrak{P}|\mathfrak{p})|.$$

En consecuencia tenemos que $|D(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Como L/K es de Galois, tenemos que $e(\sigma\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})$ y $f(\sigma\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p})$ para toda $\sigma \in G$ y si ponemos $e := e(\mathfrak{P}|\mathfrak{p})$ y $f := f(\mathfrak{P}|\mathfrak{p})$, entonces

$$[L : K] = efg$$

donde g es el número de ideales primos de \mathcal{O}_L que dividen a \mathfrak{p} :

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \quad \text{con} \quad f = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

Notemos que como $\mathcal{O}_K/\mathfrak{p}$ es un campo finito, digamos que $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_q$, $\mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_{q^f}$, entonces $\text{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ es un grupo cíclico de orden f generado por el *automorfismo de Frobenius*:

$$\varphi_{\mathfrak{p}}: \mathbb{F}_{q^f} \rightarrow \mathbb{F}_{q^f}, \quad \varphi_{\mathfrak{p}}(x) = x^q.$$

Cuando \mathfrak{p} no es ramificado se tiene que $I(\mathfrak{P}|\mathfrak{p}) = \{\text{Id}\}$ y por lo tanto existe un único $\theta \in G$ tal que $\tilde{\theta} = \varphi_{\mathfrak{p}}$. Es el automorfismo de Frobenius y se denota por: $\theta = \left[\frac{L/K}{\mathfrak{P}} \right]$.

Se tiene que $\left[\frac{L/K}{\sigma\mathfrak{P}} \right] = \sigma\theta\sigma^{-1} = \sigma \left[\frac{L/K}{\mathfrak{P}} \right] \sigma^{-1}$. Notemos que

$$D(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma D(\mathfrak{P}|\mathfrak{p})\sigma^{-1} \quad \text{y} \quad I(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma I(\mathfrak{P}|\mathfrak{p})\sigma^{-1}.$$

El *símbolo de Artin* $\left(\frac{L/K}{\mathfrak{p}}\right)$ está definido por la clase de conjugación

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{ \sigma \left[\frac{L/K}{\mathfrak{p}} \right] \sigma^{-1} \mid \sigma \in G \right\}.$$

Cuando L/K es una extensión abeliana y \mathfrak{p} es no ramificado se tiene que el símbolo de Artin consta de un elemento, esto es, $\left(\frac{L/K}{\mathfrak{p}}\right) \in G$ y satisface

$$\left(\frac{L/K}{\mathfrak{p}}\right)(x) \equiv x^q \pmod{\mathfrak{p}} \quad \forall x \in \mathcal{O}_L.$$

Definición 1.3.3. Con la notación anterior, ponemos $G_{-2} := G$, $G_{-1} := D(\mathfrak{p}|\mathfrak{p})$, $G_0 := I(\mathfrak{p}|\mathfrak{p})$ y en general para $i \geq -1$, $i \in \mathbb{Z}$, se define el i -ésimo grupo de ramificación G_i por:

$$G_i := \{\sigma \in G_{-1} \mid \sigma a - a \in \mathfrak{p}^{i+1} \quad \forall a \in \mathcal{O}_L\}.$$

Proposición 1.3.4. Las siguientes condiciones son equivalentes

- (I) $\sigma \in G_i$, $i \geq -1$, es decir, $\sigma a - a \in \mathfrak{p}^{i+1} \quad \forall a \in \mathcal{O}_L$.
- (II) $\sigma\pi - \pi \in \mathfrak{p}^{i+1}$ para un elemento $\pi \in \mathcal{O}_L$ tal que $v_{\mathfrak{p}}(\pi) = 1$.

Demostración. (i) \Rightarrow (ii): Es inmediata.

(ii) \Rightarrow (i): Sea E el campo de inercia de \mathfrak{p} , esto es, $E := L^{G_0}$. Entonces si $\mathfrak{q} := \mathfrak{p} \cap \mathcal{O}_E$, se tiene que \mathfrak{q} es totalmente ramificado en la extensión L/E . Tomamos las localizaciones $B := \mathcal{O}_{L,\mathfrak{p}} \supseteq \mathcal{O}_L$ y $A := \mathcal{O}_{E,\mathfrak{q}}$. Entonces A y B son anillos de valuación discreta y B es un A -módulo libre de rango $|G_0|$. Entonces $B = A[\pi]$. Si $a \in B$, entonces se tiene

$$a = \sum_{i=0}^{e-1} \alpha_i \pi^i, \quad e := |G_0|, \quad \text{y} \quad \alpha_i \in A.$$

Por lo tanto

$$\begin{aligned} \sigma a - a &= \sum_{i=0}^{e-1} \alpha_i (\sigma \pi^i - \pi^i) \\ &= \sum_{i=1}^{e-1} \alpha_i (\sigma\pi - \pi) (\sigma \pi^{i-1} + (\sigma \pi^{i-2}) \cdot \pi + \cdots + (\sigma \pi) \cdot \pi^{i-2} + \pi^{i-1}) \\ &\in \mathfrak{p}^{i+1} B. \end{aligned}$$

En particular, si $a \in \mathcal{O}_L$, $\sigma a - a \in \mathfrak{p}^{i+1} B \cap \mathcal{O}_L = \mathfrak{p}^{i+1}$. □

Se tiene que G_i es un subgrupo normal de $G_{-1} = D(\mathfrak{p}|\mathfrak{p})$, $G_{i+1} \subseteq G_i$. Además para i suficientemente grande tenemos que $G_i = \{\text{Id}\}$.

Para $\sigma \in G_{-1}$, $\sigma \neq \text{Id}$, existe i tal que $\sigma \in G_i \setminus G_{i+1}$. Se define $i_{G_{-1}}(\sigma) := i$. Si $\sigma = \text{Id}$ definimos $i_{G_{-1}}(\sigma) = \infty$. Notemos que $i_{G_{-1}}(\sigma) \geq i + 1$ si y sólo si $\sigma \in G_i$. Además se tiene

$$\sum_{\sigma \neq \text{Id}} i_{G_{-1}}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1).$$

La conexión con el diferente la obtenemos del siguiente resultado:

Teorema 1.3.5. *Sean \mathfrak{P} y \mathfrak{p} como antes. Sea $s \geq 0$ la potencia de \mathfrak{P} que aparece en $\mathfrak{D}_{L/K}$. Entonces*

$$s = \sum_{\sigma \neq \text{Id}} i_{G_{-1}}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1). \quad \square$$

Corolario 1.3.6. *Se tiene que \mathfrak{P} es salvajemente ramificado si y solamente si $G_1 \neq \{\text{Id}\}$.* \square

Ahora consideremos un subgrupo H de G . Sean $E := L^H$, el campo fijo de H , y $\mathfrak{q} := \mathfrak{P} \cap E$. Entonces los grupos de ramificación de H satisfacen:

Proposición 1.3.7. *Para $\sigma \in H$ se tiene $i_H(\sigma) = i_G(\sigma)$ y $H_i = G_i \cap H$ para toda $i \geq -1$.* \square

Ahora veamos algunas otras propiedades de los grupos de inercia que usaremos más adelante, en particular en la demostración del Teorema de Kronecker–Weber.

Sea E un campo numérico, \mathcal{O}_E su anillo de enteros. Sea \mathfrak{P} un ideal primo no cero de \mathcal{O}_E . Sea $S := \mathcal{O}_E \setminus \mathfrak{P}$ el complemento de \mathfrak{P} y $\hat{\mathcal{O}}_E := S^{-1}\mathcal{O}_E = (\mathcal{O}_E)_{\mathfrak{P}}$ la localización de \mathcal{O}_E en \mathfrak{P} . Se tiene que $\hat{\mathcal{O}}_E = \{\frac{\alpha}{\beta} \in E \mid \alpha, \beta \in \mathcal{O}_E, \beta \notin \mathfrak{P}\}$. Entonces $\hat{\mathcal{O}}_E$ es un anillo local con ideal máximo $\hat{\mathfrak{P}} := \mathfrak{P}\hat{\mathcal{O}}_E = \{\frac{\alpha}{\beta} \in E \mid \alpha \in \mathfrak{P}, \beta \in \mathcal{O}_E \setminus \mathfrak{P}\}$ y las unidades de $\hat{\mathcal{O}}_E$ son $\hat{\mathcal{O}}_E^* = \hat{\mathcal{O}}_E \setminus \hat{\mathfrak{P}}$. Sean

$$U^{(0)} = \hat{\mathcal{O}}_E^* \quad \text{y} \quad U^{(n)} = 1 + \hat{\mathfrak{P}}^n \subseteq \hat{\mathcal{O}}_E^*, \quad n \geq 1.$$

Entonces $U^{(i)}$ es cerrado con la multiplicación para $i \geq 0$ y de hecho si $v_{\mathfrak{P}}$ es la valuación $\hat{\mathfrak{P}}$ -ádica $U^{(i)} = \{x \in \hat{\mathcal{O}}_E^* \mid v_{\mathfrak{P}}(x - 1) \geq i\}$. Notemos que para $i \geq 1$, $U^{(i)}/U^{(i+1)}$, el cual entenderemos como las clases de equivalencia

$$1 + x \sim 1 + y \iff x - y \in U^{(i+1)},$$

es un grupo pues el inverso de la clase $\overline{(1+x)}$ es $\overline{(1+x)^{-1}} = \overline{1-x}$, lo cual se sigue del hecho de que $(1+x)(1-x) = 1 - x^2 \in U^{(i+1)}$.

Proposición 1.3.8. *Sea E cualquier campo numérico. Entonces*

- (1) $U^{(0)}/U^{(1)} \cong (\mathcal{O}_E/\mathfrak{P})^*$.
 (2) $U^{(i)}/U^{(i+1)} \cong \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1} \cong \mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \mathcal{O}_E/\mathfrak{P}$ para $i \geq 1$.

Demostración. (1) Sea $\varphi: U^{(0)} \rightarrow (\hat{\mathcal{O}}_E/\hat{\mathfrak{P}})^*$, $\varphi(x) = x \bmod \hat{\mathfrak{P}}$. Entonces φ es un epimorfismo de grupos abelianos multiplicativos. Además $\text{núc } \varphi = \{x \in \hat{\mathcal{O}}_E^* \mid \varphi(x) = x \bmod \hat{\mathfrak{P}} \equiv 1 \bmod \hat{\mathfrak{P}}\} = U^{(1)}$. Por tanto $U^{(0)}/U^{(1)} \cong (\mathcal{O}_E/\mathfrak{P})^*$.

(2) Sea $\psi: \hat{\mathfrak{P}}^i: U^{(i)}$, $\psi_i(x) = 1 + x$. Entonces ψ es un mapeo biyectivo que no es homomorfismo tal que compuesto con la proyección natural $U^{(i)} \rightarrow U^{(i)}/U^{(i+1)}$ nos da una función suprayectiva $\tilde{\psi}_i: \hat{\mathfrak{P}}^i \rightarrow U^{(i)}/U^{(i+1)}$ donde tanto $\hat{\mathfrak{P}}^i$ como $U^{(i)}/U^{(i+1)}$ son grupos abelianos. Sean $x, y \in \hat{\mathfrak{P}}^i$, entonces $\tilde{\psi}_i(x+y) = 1 + (x+y) \bmod U^{(i+1)}$ y

$$\tilde{\psi}_i(x)\tilde{\psi}_i(y) = (1+x)(1+y) \bmod U^{(i+1)} = 1 + (x+y) + (xy) \bmod U^{(i+1)}.$$

Ahora bien, puesto que $x, y \in \hat{\mathfrak{P}}^i$ con $i \geq 1$ y en particular $i+1 \leq 2i$, entonces $xy \in \hat{\mathfrak{P}}^{2i} \subseteq \hat{\mathfrak{P}}^{i+1}$ y por tanto $1 + xy \equiv 1 \bmod U^{(i+1)}$. Se sigue que $\tilde{\psi}_i(xy) = \tilde{\psi}_i(x)\tilde{\psi}_i(y)$.

Entonces $\tilde{\psi}_i$ es un epimorfismo de grupos con $\text{núc } \tilde{\psi}_i = \hat{\mathfrak{P}}^{i+1}$ de donde obtenemos que $U^{(i)}/U^{(i+1)} \cong \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1}$.

Como siguiente paso probemos que $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1}$ para $i \geq 1$.

Sea $\mathfrak{P}^i \xrightarrow{\alpha} \hat{\mathfrak{P}}^i \xrightarrow{\beta} \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1}$ los homomorfismos naturales $\alpha(x) = \frac{x}{1}$ y $\beta(y) = y \bmod \hat{\mathfrak{P}}^{i+1}$. Puesto que claramente tenemos que $\text{núc}(\beta \circ \alpha) = \mathfrak{P}^{i+1}$, basta probar que $\beta \circ \alpha$ es suprayectiva. Sea $\frac{x}{t} \in \hat{\mathfrak{P}}^i$, es decir $x \in \hat{\mathfrak{P}}^i$, $t \notin \mathfrak{P}$. Entonces puesto que \mathfrak{P} es maximal y $t \notin \mathfrak{P}$, se tiene que $(t) + \mathfrak{P} = \mathcal{O}_E$ y por tanto $\mathfrak{P}^i(t) + \mathfrak{P}^{i+1} = \mathfrak{P}^i$. En particular existen $a \in \mathfrak{P}^i$ y $z \in \mathfrak{P}^{i+1}$ tales que $at + z = x$ y $\frac{x}{t} - \frac{a}{1} = \frac{z}{t} \in \hat{\mathfrak{P}}^{i+1}$.

Por tanto $(\beta \circ \alpha)(a) = \frac{a}{1} \bmod \hat{\mathfrak{P}}^{i+1} = \frac{x}{t} \bmod \hat{\mathfrak{P}}^{i+1}$ y $\beta \circ \alpha$ es suprayectiva probando que $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1}$ para $i \geq 0$.

Para $i = 0$, $\hat{\mathcal{O}}_E/\hat{\mathfrak{P}} \cong \mathcal{O}_E/\mathfrak{P}$. Finalmente probaremos que $\hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1} \cong \hat{\mathcal{O}}_E/\hat{\mathfrak{P}}$ y con esto terminaremos la demostración. Puesto que $\hat{\mathcal{O}}_E$ es un anillo de valuación y $\hat{\mathfrak{P}} = (\pi)$ es principal, el mapeo

$$\begin{aligned} \hat{\mathcal{O}}_E &\rightarrow \hat{\mathfrak{P}}^i \rightarrow \hat{\mathfrak{P}}^i/\hat{\mathfrak{P}}^{i+1} \\ x &\mapsto x\pi^i \mapsto x\pi^i \bmod \hat{\mathfrak{P}}^{i+1} \end{aligned}$$

es un epimorfismo de grupos con núcleo $\hat{\mathfrak{P}}^i$. □

La conexión que tenemos entre los grupos de ramificación y los grupos $U^{(i)}/U^{(i+1)}$ nos lo da el siguiente resultado.

Proposición 1.3.9. *Sea K/\mathbb{Q} una extensión finita de Galois con grupo de Galois G . Sean p un número primo racional y \mathfrak{P} un primo en \mathcal{O}_K sobre p .*

Sea $G_{-1} = D(\mathfrak{P}|p)$ el grupo de descomposición, $G_0 = I(\mathfrak{P}|p)$ el grupo de inercia y G_i , $i \geq 1$ los grupos de ramificación. Sean $U^{(i)} = 1 + \hat{\mathfrak{P}}^i$, $i \geq 0$, con $U^{(0)} = \hat{\mathcal{O}}_K^*$. Sea $\pi \in \mathcal{O}_E$ un elemento primo de $\hat{\mathfrak{P}}$, es decir, $(\pi) = \hat{\mathfrak{P}}$ para lo cual es suficiente seleccionar $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Entonces $\sigma \in G_i \iff \sigma(\pi)/\pi \in U^{(i)}$, $i \geq 0$.

Demostración. Recordemos que $\sigma \in G_i \iff \sigma\pi - \pi \in \mathfrak{P}^{i+1}$ (Proposición 1.3.4). Por lo tanto para $\sigma \in G_i \iff \sigma\pi - \pi \in \hat{\mathfrak{P}}^{i+1} \iff \frac{\sigma\pi}{\pi} - 1 \in \hat{\mathfrak{P}}^i$ siendo esto último equivalente a que $\frac{\sigma\pi}{\pi} \in 1 + \hat{\mathfrak{P}}^i = U^{(i)}$. \square

Proposición 1.3.10. *Se tiene para $i \geq 0$ que el mapeo*

$$\varphi: G_i/G_{i+1} \rightarrow U^{(i)}/U^{(i+1)}, \quad \varphi(\sigma \bmod G_{i+1}) := \sigma\pi/\pi \bmod U^{(i+1)}$$

donde π es un elemento primo de \mathfrak{P} , $v_{\mathfrak{P}}(\pi) = 1$, es un monomorfismo de grupos que es independiente de π . En particular G_i/G_{i+1} es un p -grupo elemental abeliano donde p es la característica de $\mathcal{O}_K/\mathfrak{P}$.

Demostración. Sea π_1 otro elemento primo, por lo que $\pi_1 = \alpha\pi$ con α una unidad. Por lo tanto

$$\frac{\sigma\pi_1}{\pi_1} = \frac{\sigma\pi}{\pi} \cdot \frac{\sigma\alpha}{\alpha}.$$

Si $\sigma \in G_i$, $\sigma\alpha - \alpha \in \mathfrak{P}^{i+1}$ lo cual implica que $\frac{\sigma\alpha}{\alpha} - 1 \in U^{(i+1)}$ lo cual demuestra que φ no depende del elemento primo π .

Sean ahora $\sigma, \theta \in G_i$, entonces

$$\frac{\sigma\theta(\pi)}{\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\theta\pi}{\pi} \cdot \frac{\sigma u}{u}, \quad u = \frac{\theta\pi}{\pi}.$$

Puesto que u es una unidad, la observación anterior muestra que $\frac{\sigma u}{u} \in U^{(i+1)}$ y por lo tanto $\varphi(\sigma\theta) = \varphi(\sigma)\varphi(\theta)$ y φ es un homomorfismo de grupos. Finalmente, si $\varphi(\sigma) = 1$, entonces $\frac{\sigma\pi}{\pi} \in U^{(i+1)}$. Por la Proposición 1.3.9 se sigue que $\sigma \in G_{i+1}$ por lo que φ es inyectiva. \square

Notemos que la Proposición 1.3.10 prueba que G_i/G_{i+1} es elemental abeliano para $i \geq 0$ y por tanto G_1 es un p -grupo, donde p es la característica de los campos residuales $\mathcal{O}_L/\mathfrak{P}$, $\mathcal{O}_K/\mathfrak{p}$ y $G_0/G_1 \subseteq (\mathcal{O}_L/\mathfrak{P})^*$, es decir, G_0/G_1 es un grupo cíclico. En particular

Corolario 1.3.11. *Se tiene que $G_{-1} = D(\mathfrak{P}|\mathfrak{p})$ es un grupo soluble, G_0/G_1 es cíclico y G_1 es un p -grupo. Si $\mathfrak{P}|\mathfrak{p}$ es moderadamente ramificado, entonces G_0 es cíclico. Finalmente G_i/G_{i+1} es un p -grupo elemental abeliano para $i \geq 1$. \square .*

Un resultado que necesitaremos para demostrar el Teorema de Kronecker-Weber es el siguiente.

Proposición 1.3.12. *Supongamos que G_{-1}/G_1 es un grupo abeliano. Entonces si $\varphi: G_0/G_1 \rightarrow U^{(0)}/U^{(1)} \cong (\mathcal{O}_K/\mathfrak{p})^*$ es el mapeo dado en la Proposición 1.3.10, se tiene que $\text{im } \varphi \subseteq (\mathbb{Z}/p\mathbb{Z})^*$.*

Demostración. Sea $\sigma \in G_0$ y supongamos que $\varphi(\bar{\sigma}) = \alpha \in (\mathcal{O}_K/\mathfrak{p})^*$, es decir, $\varphi(\bar{\sigma}) = \frac{\sigma\pi}{\pi} \text{ mód } \mathfrak{p} = \alpha$, esto es, $\sigma\pi = \alpha\pi \text{ mód } \mathfrak{p}$. Sea $\theta \in G_{-1}$ arbitrario y sea $\pi_1 := \theta^{-1}(\pi)$, el cual es un elemento primo para \mathfrak{p} , entonces se tiene

$$\sigma\theta^{-1}(\pi) \equiv \alpha\theta^{-1}(\pi) \text{ mód } \mathfrak{p}.$$

Por ser G_{-1}/G_1 abeliano tenemos

$$(\theta\sigma\theta^{-1})(\pi) \equiv \sigma\pi \equiv \theta(\alpha)\pi \text{ mód } \mathfrak{p} \equiv \alpha\pi \text{ mód } \mathfrak{p}.$$

Por tanto $\theta(\alpha) \equiv \alpha \text{ mód } \mathfrak{p}$ para toda $\theta \in G_{-1}/G_1$. Se sigue que α es invariante bajo $G_{-1}/G_0 \cong \text{Gal}((\mathcal{O}_K/\mathfrak{p}) : (\mathbb{Z}/p\mathbb{Z}))$ y por tanto $\alpha \in \mathbb{Z}/p\mathbb{Z}$. \square

1.4. Primos infinitos

Sea K un campo numérico, $[K : \mathbb{Q}] = n = r_1 + 2r_2$. Sean

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+1}, \dots, \bar{\sigma}_{r_1+r_2}$$

los r_1 encajes reales de K y los $2r_2$ encajes complejos:

$$\begin{aligned} \sigma_i: K &\longrightarrow \mathbb{R}, & 1 \leq i \leq r_1, \\ \sigma_{r_1+j}: K &\longrightarrow \mathbb{C}, & 1 \leq j \leq r_2, \quad \sigma_{r_1+j}(K) \not\subseteq \mathbb{R}. \end{aligned}$$

Sea $||$ el valor absoluto usual de \mathbb{C} . Definimos los siguientes valores absolutos definidos sobre K :

$$|x|_{\sigma_i} := |\sigma_i x|, \quad 1 \leq i \leq r_1 + r_2, \quad \text{donde} \quad |\sigma_{r_1+j} x| = |\bar{\sigma}_{r_1+j} x|.$$

Definición 1.4.1. Los valores absolutos $\{|\sigma_i|\}_{1 \leq i \leq r_1+r_2}$ son los *primos infinitos* de K . Los valores absolutos $\{|\sigma_i|\}_{1 \leq i \leq r_1}$ son los *primos infinitos reales* y $\{|\sigma_{r_1+j}|\}_{1 \leq j \leq r_2}$ son los *primos infinitos complejos*.

En \mathbb{Q} únicamente existe un primo infinito, el cual es real, y corresponde al valor absoluto usual. Para $[K : \mathbb{Q}] = n = r_1 + 2r_2$ se tienen $r_1 + r_2$ primos infinitos, r_1 reales y r_2 complejos.

Notemos que esta definición de hecho generaliza el concepto de primo, pues si \mathfrak{p} es un primo de \mathcal{O}_K , a \mathfrak{p} le podemos asociar su valuación: si $x \in K^*$, $x\mathcal{O}_K = \langle x \rangle = \mathfrak{p}^n \mathfrak{a}$ con $(\mathfrak{p}, \mathfrak{a}) = 1$, $n \in \mathbb{Z}$. Entonces $v_{\mathfrak{p}}(x) = n$ y definimos el *valor absoluto \mathfrak{p} -ádico*:

$$|x|_{\mathfrak{p}} := p^{-f^n} \quad \text{donde} \quad \mathfrak{p} \cap \mathbb{Q} = \langle p \rangle, \quad n_{L/\mathbb{Q}}\mathfrak{p} = p^f,$$

es decir, donde f es el grado de inercia.

En otras palabras, $|x|_{\mathfrak{p}} = p^{-f^n} = (N_{K/\mathbb{Q}}\mathfrak{p})^{v_{\mathfrak{p}}(x)}$. Se define $|0|_{\mathfrak{p}} = 0$. Este valor absoluto es no *arquimideano*:

$$|x + y|_{\mathfrak{p}} \leq \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\}$$

y los valores absolutos $|\cdot|_{\sigma_i}$ son arquimideanos. Resumiendo, podemos pensar en “primos” de K como un valor absoluto de K .

Ahora consideremos L/K una extensión de campos numéricos. Sea $\omega: L \rightarrow \mathbb{C}$ un encaje de L y sea $\omega|_K = \sigma$, $\sigma: K \rightarrow \mathbb{C}$ es un encaje de K . Notemos que si ω es real, σ necesariamente es real, pero si ω es complejo, entonces σ puede ser real o complejo.

Definición 1.4.2. Con la notación anterior, decimos que ω (o σ) es *ramificado* si σ es real y ω es complejo y definimos que el índice de ramificación como 2: $e(\omega|\sigma) = 2$. Esto se hace pensando en que $[\mathbb{C} : \mathbb{R}] = 2$ o en que $\omega|_K = \bar{\omega}|_K = \sigma$.

En el caso de que ω y σ sean ambos reales o ambos complejos, entonces definimos el índice de ramificación como 1: $e(\omega|\sigma) = 1$.

En cualquier caso, el grado de inercia lo definimos como 1: $f(\omega|\sigma) = 1$ siempre.

$$\text{Se tiene } e(\omega|\sigma)f(\omega|\sigma) = \begin{cases} 2 & \text{si } \omega \text{ es complejo y } \sigma \text{ es real} \\ 1 & \text{en otro caso.} \end{cases}$$

En particular, si fijamos $\sigma: K \rightarrow \mathbb{C}$ un encaje. σ tiene $[L : K]$ extensiones a encajes $\omega: L \rightarrow \mathbb{C}$. Si ω y $\bar{\omega}$ son dos complejos conjugados de estos encajes, ω y $\bar{\omega}$ los consideramos los mismos y denotamos a cualquier extensión ω por $\omega|\sigma$.

Entonces

$$\sum_{\omega|\sigma} e(\omega|\sigma)f(\omega|\sigma) = [L : K].$$

Esta fórmula es exactamente la misma fórmula que para los primos finitos:

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}) = [L : K]$$

donde \mathfrak{p} es un primo de \mathcal{O}_K y $\mathfrak{P}|\mathfrak{p}$ recorre los primos de \mathcal{O}_L sobre \mathfrak{p} .

Terminamos esta sección mencionando el Teorema de Hilbert sobre la máxima extensión abeliana no ramificada de un campo.

Teorema 1.4.3 (Campo de clase de Hilbert). *Sea K un campo finito y sea C_K su grupo de clases de ideales de K . Sea H_K la máxima extensión abeliana de K no ramificada en ningún primo, finito o infinito. Entonces H_K es una extensión finita y de Galois de K con grupo de Galois isomorfo a C_K : $\text{Gal}(H_K/K) \cong C_K$.* \square

Teoría de Galois infinita

2.1. Límites directos y límites inversos

Primero recordemos algunos conceptos generales. Sea A un anillo conmutativo con unidad.

Definición 2.1.1. Un *conjunto dirigido* I es un conjunto no vacío parcialmente ordenado tal que para cualesquiera $i, j \in I$ existe $k \in I$ tal que $i \leq k$ y $j \leq k$.

Sea I un conjunto dirigido y se $\{M_i\}_{i \in I}$ un conjunto de A -módulos. Si para cualesquiera $i, j \in I$ con $i \leq j$ existe $\varphi_{i,j}: M_i \rightarrow M_j$ un A -homomorfismo tal que

- (I) $\varphi_{ii} = \text{Id}_{M_i}$ para toda $i \in I$,
- (II) $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$ para cualesquiera $i \leq j \leq k$,

entonces decimos que $\{M_i, \varphi_{ij}, I\}_{i,j \in I, i \leq j}$ forman un *sistema directo* sobre I .

Definición 2.1.2. Si $\{M_i, \varphi_{ij}, I\}_{i,j \in I, i \leq j}$ es un sistema directo, el *límite directo* se define como el A -módulo

$$\varinjlim_{i \in I} M_i =: M$$

definido por P/N donde $P = \bigoplus_{i \in I} M_i$ y $N = \langle m_i - \varphi_{ij}(m_i) \mid i \in I, m_i \in M, i \leq j \rangle$.

Se tiene que existe $h_i: M_i \rightarrow M$ dado por $h_i = \pi \circ \mu_i$ donde $\mu_i: M_i \rightarrow P$ es el encaje natural y $\pi: P \rightarrow P/N$ es la proyección natural. En otras palabras

$$h_i(x) := (\xi_j)_{j \in I} \text{ mód } N \quad \text{donde} \quad \xi_j = \begin{cases} 0 & \text{si } j \neq i \\ x & \text{si } j = i. \end{cases}$$

Se tiene que $h_i = h_j \circ \varphi_{ij}$ para $i \leq j, i, j \in I$.

Enunciamos en el siguiente resultado todas las propiedades que necesitamos.

Teorema 2.1.3. Sea I un conjunto dirigido, $\{M_i, \varphi_{ij}, I\}_{i,j \in I}$ un sistema directo y $M = \varinjlim M_i$, el límite directo. Sean $h_i: M_i \rightarrow M$ los homomorfismos naturales. Entonces

- (1) Dado $m \in M$, existen $i \in I$ y $x \in M_i$ tales que $m = h_i(x)$.
- (2) Todo elemento que es 0 en M , es que era eventualmente 0 en los M_i 's. Esto es, si $h_i(x) = 0$ con $x \in M_i$, entonces existe $j \geq i$ tal que $\varphi_{ij}(x) = 0 \in M_j$.
- (3) M satisface la siguiente propiedad universal: Sea N un A -módulo tal que para toda $i \in I$ existe $\theta_i: M_i \rightarrow N$ un homomorfismo de A -módulos tal que

$$\begin{array}{ccc} M_i & \xrightarrow{\varphi_{ij}} & M_j \\ & \searrow \theta_i & \swarrow \theta_j \\ & N & \end{array} \quad \theta_j \circ \varphi_{ij} = \theta_i \quad \text{para toda } i \leq j.$$

Entonces existe un único homomorfismo $\theta: M \rightarrow N$ tal que

$$\begin{array}{ccc} M_i & \xrightarrow{h_i} & M \\ & \searrow \theta_i & \swarrow \theta \\ & N & \end{array} \quad \theta \circ h_i = \theta_i \quad \text{para toda } i \in I.$$

- (4) M está caracterizado por la propiedad universal de (3).
- (5) Si $\{M_i\}_{i \in I}$ es una familia de submódulos de un A -módulo N tal que para cualesquiera $i, j \in I$ existe $k \in I$ tal que $M_i + M_j \subseteq M_k$. Se define $i \leq j$ en I si y sólo si $M_i \subseteq M_j$. Entonces I es un sistema dirigido y se define $\varphi_{ij}: M_i \rightarrow M_j$ como el encaje natural cuando $i \leq j$. Entonces

$$M = \varinjlim_{i \in I} M_i = \sum_{i \in I} M_i = \bigcup_{i \in I} M_i$$

donde $h_i: M_i \rightarrow M$ es el encaje natural.

Demostración. [4, pags. 32–33]. □

Estamos interesados en el caso especial de una extensión de Galois de campos. Podemos considerar a los campos como \mathbb{Z} -módulos. Sea L/K una extensión cualquiera de Galois, no necesariamente finita. Para cada $\alpha \in L$, $K(\alpha)/K$ es una extensión finita. Entonces $L = \bigcup_{\alpha \in L} K(\alpha) = \varinjlim_{\alpha \in L} K(\alpha)$, donde los homomorfismos están dados por $K(\alpha) \rightarrow K(\beta)$ el encaje natural para $K(\alpha) \subseteq K(\beta)$.

Notemos que con esta notación, el conjunto dirigido es $I := \{K(\alpha) \mid \alpha \in L\}$ donde se define $K(\alpha) \leq K(\beta) \iff K(\alpha) \subseteq K(\beta)$. Veamos cual es la conexión con los grupos de Galois.

Para este fin, consideremos ahora *límites inversos*. Sea I un conjunto dirigido. Para cada $i \in I$ consideremos un objeto A_i , el cual puede ser un grupo, un espacio topológico, un anillo, un módulo, un conjunto, etc. Nuestro interés será fundamentalmente en considerar A_i un grupo finito con la topología discreta.

Definición 2.1.4. Un *sistema inverso* $\{A_i, \phi_{ji}, I\}_{i,j \in I, i \leq j}$ es un sistema tal que $\phi_{ji}: A_j \rightarrow A_i$ son morfismos para $i \leq j$ tales que:

- (1) $\phi_{ii} = \text{Id}_{A_i}$ para toda $i \in I$.
- (2) $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ para $i \leq j \leq k$,

$$\begin{array}{ccc} A_k & \xrightarrow{\phi_{kj}} & A_j \\ & \searrow \phi_{ki} & \swarrow \phi_{ji} \\ & A_i & \end{array}$$

(por *morfismo* entendemos homomorfismo si los objetos son grupos, anillos, campos, módulos o cualquier otra estructura algebraica; función continua si los objetos son espacios topológicos, homomorfismo continuo si los objetos son grupos o anillos topológicos y simples funciones si los A_i 's son simplemente conjuntos).

Si $\{A_i, \phi_{ji}, I\}_{i,j \in I, i \leq j}$ es un sistema inverso, entonces decimos que $(X, \varphi_i)_{i \in I}$ es un *límite inverso* del sistema si $\varphi_i: X \rightarrow A_i$ son morfismos tales que

$$\phi_{ji} \circ \varphi_j = \varphi_i \quad \text{para } i \leq j \quad \begin{array}{ccc} X & \xrightarrow{\varphi_j} & A_j \\ & \searrow \varphi_i & \swarrow \phi_{ji} \\ & A_i & \end{array}$$

y si $(Y, \mu_i)_{i \in I}$ es otro sistema tal que $\mu_i: Y \rightarrow A_i$ son morfismos tales que

$$\begin{array}{ccc} Y & \xrightarrow{\mu_i} & A_j \\ & \searrow \mu_i & \swarrow \varphi_{ij} \\ & A_i & \end{array} \quad \varphi_{ij} \circ \mu_j = \mu_i \quad \text{para toda } i \leq j$$

entonces existe un único morfismo $\xi: Y \rightarrow X$ tal que

$$\begin{array}{ccc}
Y & \xrightarrow{\xi} & X \\
\mu_i \searrow & & \swarrow \varphi_i \\
& A_i &
\end{array}
\quad \varphi_i \circ \xi = \mu_i \quad \text{para toda } i \in I.$$

Escribimos

$$X = \varprojlim_{i \in I} A_i = \varprojlim_i A_i = \varprojlim A_i.$$

Teorema 2.1.5. *Dado un sistema inverso $\{A_i, \phi_{ji}, I\}_{i,j \in I}$ existe el límite inverso $(X, \varphi_i)_{i \in I}$, $X = \varprojlim_{i \in I} A_i$. Se tiene que $(X, \varphi_i)_{i \in I}$ es único salvo isomorfismo.*

Más aún $(X, \varphi_i)_{i \in I}$ se puede realizar como las “sucesiones coherentes” de $B := \prod_{i \in I} A_i$, el producto directo, es decir

$$X = \{(a_i)_{i \in I} \in B \mid a_i = \phi_{ji}(a_j) \text{ para toda } i, j \in I, i \leq j\}$$

donde $\phi_i: X \rightarrow A_i$ es la i -ésima proyección.

Demostración. Se puede consultar la demostración en [70, Capítulo 11] o [54]. Aquí la volvemos a presentar.

Primero veamos la unicidad. Si $(Z, \theta_i)_{i \in J}$ es otro límite inverso, entonces existe mapeos únicos $\alpha: X \rightarrow Z$, $\beta: Z \rightarrow X$ tales que los siguientes diagramas conmutan:

$$\begin{array}{ccccc}
X & \xrightarrow{\alpha} & Z & \xrightarrow{\beta} & X \\
& \searrow \varphi_i & \downarrow \theta_i & \swarrow \varphi_i & \\
& & A_i & &
\end{array}$$

Entonces $\beta \circ \alpha$ y Id_X satisfacen que $\varphi_i \circ (\beta \circ \alpha) = \varphi_i = \varphi_i \circ (\text{Id}_X)$. Por la unicidad tenemos que $\beta \circ \alpha = \text{Id}_X$. Análogamente tenemos $\alpha \circ \beta = \text{Id}_Z$. Esto prueba que α y β son isomorfismos inversos uno del otro entre X y Z .

Para ver la existencia, sea $B := \prod_{i \in I} A_i$. Se define $X := \{(a_i)_{i \in I} \in B \mid \phi_{kj}(a_k) = a_j \text{ si } j \leq k\}$ (B se considera con las operaciones entrada por entrada en el caso de grupos, anillos, campos, módulos, etc. o con la topología producto en el caso de espacios topológicos). Sea $\pi_i: B \rightarrow A_i$ la proyección y sea $\varphi_i: X \rightarrow A_i$, $\varphi_i := \pi_i|_X$. Se tiene que

$$(\phi_{ij} \circ \varphi_j) = ((a_k)_{k \in I}) = \phi_{ij}(a_j) = a_i = \varphi_i((a_k)_{k \in I})$$

para todo $(a_k)_{k \in I} \in X$. Si $(Y, \xi_i)_{i \in I}$ es tal que $\xi_i: Y \rightarrow A_i$ satisface $\phi_{ji} \circ \xi_j = \xi_i$ para $i \leq j$, sea $\xi: Y \rightarrow X$ dada por $\xi(y) := (\xi_i(y))_{i \in I}$. Entonces ξ está bien definido puesto que $(\varphi_i \circ \xi)(y) = \varphi_i((\xi_k(y))_{k \in I})$ de tal forma que $\xi(y) \in X$. Por tanto X es un límite inverso de $\{A_i, \phi_{ji}, I\}$. \square

Observación 2.1.6. Si para cada $i \in I$, A_i es un espacio topológico Hausdorff, damos a $A := \prod_{i \in I} A_i$ la topología producto y $\lim_{\leftarrow} A_i$ es un espacio topológico con la topología inducida. Siempre supondremos que los mapeos ϕ_{ji} son continuos. Ahora, las funciones ϕ_i son siempre continuas pues si U es un abierto de A_i , tenemos que $\phi_i^{-1}(U) = \pi_i^{-1}(U) \cap \lim_{\leftarrow} A_i$ y $\pi_i^{-1}(U)$ es un conjunto abierto en A por la definición de la topología producto.

Se tiene mucho más. Si V es un conjunto abierto de $X = \lim_{\leftarrow} A_i$, veremos que V contiene a algún conjunto de la forma $\phi_k^{-1}(U_k)$ para algún conjunto abierto U_k de A_k y algún $k \in I$. Se tiene que V está generado por uniones e intersecciones finitas de conjuntos de la forma $\pi_j^{-1}(U_j) \cap X$, por lo que basta verificar que $\phi_i^{-1}(U_i) \cap \phi_j^{-1}(U_j) = \phi_k^{-1}(U_k)$ para algún k .

Sea $k \geq i, j$ y sea $U_k := \phi_{kj}^{-1}(U_j) \cap \phi_{ki}^{-1}(U_i)$. Entonces

$$\phi_k^{-1}(U_k) = \phi_k^{-1}(\phi_{kj}^{-1}(U_j)) \cap \phi_k^{-1}(\phi_{ki}^{-1}(U_i)) = \phi_j^{-1}(U_j) \cap \phi_i^{-1}(U_i).$$

Observación 2.1.7. Se puede probar que si $\{A_i, \phi_{ji}, I\}_{\substack{i, j \in I \\ i \leq j}}$ es un sistema inverso de espacios compactos Hausdorff no vacíos, entonces $X \neq \emptyset$.

También en general, si los A_i son espacios topológicos (y posiblemente algo más) consideramos a $B = \prod_{i \in I} A_i$ con la topología producto. Entonces X es un subespacio cerrado de B (Proposición 2.1.8). En particular, si cada A_i es compacto, entonces B es compacto y por lo tanto X es compacto.

Proposición 2.1.8. X es cerrado en B .

Demostración. Sea $(a_i)_{i \in I} \in B \setminus X$. Entonces existen $i \leq j$ tales que $\phi_{ji}(a_j) \neq a_i$. Por ser A_i Hausdorff existen vecindades abiertas U de $\phi_{ji}(a_j)$ y V de a_i tales que $U \cap V = \emptyset$. Sea $W := \phi_{ij}^{-1}(U)$, el cual es un abierto de A_j . El conjunto $\tilde{U} = V \times W \times \prod_{k \neq i, j} A_k \subseteq B$ es un abierto y $(a_i)_{i \in I} \in \tilde{U}$. Puesto que $\phi_{ji}(W) \subseteq U$ y $U \cap V = \emptyset$ se tiene que $\tilde{U} \cap X = \emptyset$ lo cual prueba que $B \setminus X$ es abierto y que X es cerrado. \square

Como mencionamos anteriormente, estamos interesados en grupos de Galois, por ello recordamos la siguiente definición.

Definición 2.1.9. Un grupo de G se llama *grupo topológico* si G es un espacio topológico tal que las operaciones de grupo

$$\begin{aligned} \circ: G \times G &\rightarrow G & \text{y} & & i: G &\rightarrow G \\ (x, y) &\mapsto xy & & & x &\mapsto x^{-1} \end{aligned}$$

son funciones continuas.

Cuando G sea un grupo finito, siempre le daremos a G la topología discreta. En general tenemos:

Proposición 2.1.10. *Un grupo topológico G es Hausdorff si y solamente si la identidad de G , $\{e\}$ es cerrada en G .*

Demostración. Si G es Hausdorff, los puntos son cerrados.

Recíprocamente, si $\{e\}$ es un conjunto cerrado en G , entonces $\mu^{-1}(\{e\}) \subseteq G \times G$ es un conjunto cerrado donde $\mu: G \times G \rightarrow G$ está dada por $\mu(x, y) = xy^{-1}$. Ahora bien, μ es una función continua por ser la composición de las funciones continuas $(\text{Id}, i): G \times G \rightarrow G \times G$, $(\text{Id}, i)(x, y) = (x, y^{-1})$ y la multiplicación. Ahora, $\mu^{-1}(\{e\}) = \{(x, x) \mid x \in G\} = \Delta$. Sabemos en general que un espacio topológico X es Hausdorff si y solamente si $\Delta = \{(x, x) \mid x \in X\}$ es cerrado en $X \times X$. Por lo tanto G es Hausdorff. \square

Otra observación es que no solamente $\{e\}$ caracteriza si G es Hausdorff o no, sino que la topología misma de G está determinada por las vecindades de $\{e\}$. Esto se sigue de que si $g \in G$ está fijo, entonces $\xi_g: G \rightarrow G$ dada por $\xi_g(h) = gh$ es un homeomorfismo de espacios topológicos pues ξ_g es continua y $\xi_g^{-1} = \xi_{g^{-1}}$. Además $\xi_g(e) = g$. Por lo tanto W es un vecindad de g si y solamente si $g^{-1}W = \xi_{g^{-1}}(W)$ es una vecindad de $\{e\}$.

Una pregunta que contestaremos a continuación es: ¿Qué grupos G pueden ser grupos de Galois de alguna extensión de campos? Sabemos que si G es finito, entonces G es el grupo de Galois de una extensión de campos L/K . Recordemos rápidamente su demostración para ver más adelante su contraparte infinita.

Sea k cualquier campo y sea $n \in \mathbb{N}$ tal que G es subgrupo del grupo simétrico S_n . Sean x_1, \dots, x_n variables independientes y $L := k(x_1, x_2, \dots, x_n) = \text{coc } k[x_1, x_2, \dots, x_n]$ el campo de las funciones racionales en n variables, esto es, $k[x_1, \dots, x_n]$ es el anillo de polinomios en n variables y $k(x_1, \dots, x_n)$ el campo de cocientes.

Hacemos actuar S_n sobre L de la siguiente forma. Si $\sigma \in S_n$ y si $f(x_1, \dots, x_n) \in L$, entonces

$$(\sigma \circ f)(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Al considerar G como subgrupo de S_n , se sigue del Teorema de Artin, que $L/L^G := K$ es una extensión de Galois con grupo de Galois G .

Resulta ser que no cualquier grupo infinito puede ser el grupo de Galois de alguna extensión. Por ejemplo, veremos que \mathbb{Z} no puede ser grupo de Galois de ninguna extensión de campos.

Definición 2.1.11. Un *grupo profinito* G es un grupo topológico Hausdorff compacto que contiene una base de vecindades abiertas de $\{e\}$ que consiste de subgrupos normales de G .

Observación 2.1.12. Si G es un grupo finito, a G se le da la topología discreta y con esta topología G es un grupo profinito.

La razón por la cual los grupos de la Definición 2.1.11 se llaman profinitos es debido a que son límites inversos de grupos finitos. De hecho tenemos el siguiente resultado.

Teorema 2.1.13. Sea G un grupo topológico. Las siguientes condiciones son equivalentes.

- (I) G es un grupo profinito.
- (II) G es el límite inverso de grupos finitos.
- (III) G es un grupo topológico Hausdorff compacto totalmente disconexo, es decir, las componentes conexas de G son los puntos.
- (IV) G es un grupo topológico Hausdorff compacto que tiene una base de vecindades de $\{e\}$ que consiste de subgrupos normales de G .

Demostración. Ver [70, Theorem 11.3.16, página 398]. □.

Observación 2.1.14. Notemos que un grupo profinito G es *completo*, es decir, toda sucesión de Cauchy en G converge en G .

Ejemplos 2.1.15. (1) Si G es finito, entonces G es profinito.
 (2) Sea $I := \mathbb{N}$ con orden definido por $n \leq m \iff n|m$. Sea

$$f_{m,n}: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

$$a \bmod m \mapsto a \bmod n.$$

Entonces el *anillo de Prüfer* $\hat{\mathbb{Z}}$ se define por

$$\hat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} \subseteq \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

$\hat{\mathbb{Z}}$ se llama *procíclico* por ser límite directo de grupos cíclicos finitos.

Sea $\varphi: \mathbb{Z} \rightarrow \hat{\mathbb{Z}}$, $\varphi(x) := (x \bmod n)_{n \in \mathbb{N}} \in \hat{\mathbb{Z}}$. Entonces φ es inyectivo y además $\varphi(\mathbb{Z})$ es denso en $\hat{\mathbb{Z}}$.

Por otro lado $\frac{\hat{\mathbb{Z}} \rightarrow n\hat{\mathbb{Z}}}{x \mapsto nx}$ es un isomorfismo de grupos y un homeomorfismo de espacios topológicos.

(3) Sea p un número primo. Para $n \in \mathbb{N} \cup \{0\}$ y $m \leq n$, la proyección natural $\varphi_{n,m}: \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$ define un sistema inverso.

Sea $X := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subseteq \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Definimos $\mathbb{Z}_p := \{\sum_{n=0}^{\infty} a_n p^n \mid$

$a_n \in \{0, 1, \dots, p-1\}\}$. \mathbb{Z}_p es la completación de \mathbb{Z} con la topología p -ádica, es decir, se define $|x|_p := p^{-v_p(n)}$ para $x \in \mathbb{Z}$, donde v_p es la valuación p -ádica la cual está definida como sigue: si $x \in \mathbb{Z}$, $x \neq 0$,

digamos $x = p^m b$ con b primo relativo a p y entonces $v_p(x) := m$. También se define $v_p(0) := \infty$ y $|0|_p := 0$.

Definimos

$$\mu: \mathbb{Z}_p \rightarrow X$$

$$\sum_{n=0}^{\infty} a_n p^n \mapsto \left(\sum_{n=0}^i a_n p^n \right)_{i \in \mathbb{N} \cup \{0\}}.$$

Entonces μ es un isomorfismo de anillos y por tanto $\mathbb{Z}_p \cong \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n \mathbb{Z}$

que también es un homeomorfismo de espacios topológicos.

Observación 2.1.16. Sea G un grupo profinito y sea N un subgrupo abierto y normal. Entonces $G := \cup_{x \in G} xN$. Puesto que N es abierto, xN es abierto y puesto que G es compacto, entonces la cubierta abierta $\{xN\}_{x \in G}$ tiene una subcubierta finita, es decir, existen $x_1, \dots, x_r \in G$ tales que $G = \cup_{i=1}^r x_i N$. En particular $[G : N] \leq r < \infty$ y por lo tanto N es de índice finito. Digamos que $[G : N] = t$ y $y_1 = e, \dots, y_t$ es un conjunto completo de representantes de las clases módulo N : $G = \bigsqcup_{i=1}^t y_i N$. En particular $N = G \setminus (\bigsqcup_{i=2}^t y_i N)$ es abierto, por lo que N es cerrado.

Más generalmente, si H es un subgrupo abierto de G , $\cup_{x \notin H} xH$ es abierto y por tanto $H = G \setminus \cup_{x \notin H} xH$ es cerrado. El recíproco no se cumple: $H = \{e\}$ es cerrado pero si G no es finito, H no es abierto pues G es compacto.

En resumen tenemos que si N es un subgrupo abierto y normal, entonces N es cerrado y de índice finito.

2.2. Teoría de Galois infinita

Definición 2.2.1. Dado un campo k , se denota por $G_k := \text{Gal}(\bar{k}/k)$ al grupo de Galois de \bar{k}/k donde \bar{k} es una cerradura separable de k y G_k es el *grupo absoluto de Galois de k* .

En general G_k es un grupo infinito y el Teorema de Correspondencia de Galois ya no se cumple en este caso.

Ejemplo 2.2.2. Si \mathbb{F}_p es campo finito de p elementos y si $G := G_{\mathbb{F}_p} = \text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, entonces si $H = (\varphi)$ es el grupo generado por el automorfismo de Frobenius, $\varphi: \bar{\mathbb{F}}_p \rightarrow \bar{\mathbb{F}}_p$, $\varphi(x) = x^p$ satisface que $\mathbb{F}_p = \bar{\mathbb{F}}_p^H = \bar{\mathbb{F}}_p^G$ pero $G \neq H$.

Para establecer la correspondencia de Galois debemos de proveer a G de una topología.

En general, sea L/K una extensión algebraica normal y separable de campos, es decir, una extensión de Galois. Sea $\mathcal{K} := \{K_i \mid i \in I\}$ la colección de todos los campos K_i tales que $K \subseteq K_i \subseteq L$ y K_i/K es una extensión finita de Galois. Entonces $L = \cup_{i \in I} K_i$.

Sea $G := \text{Gal}(L/K)$, $N_i := \text{Gal}(L/K_i)$, $i \in I$. Entonces $K_i = L^{N_i} = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in N_i\}$ y se tiene $N_i \triangleleft G$, $G/N_i \cong \text{Gal}(K_i/K)$ es un grupo finito.

Se define en G la *topología de Krull* definiendo $\{\sigma N_i \mid i \in I\}$ como un sistema de vecindades abiertas de $\sigma \in G$. Se tiene que la multiplicación y la inversión

$$\begin{aligned} \varphi: G \times G &\rightarrow G, & i: G &\rightarrow G \\ (\sigma, \psi) &\mapsto \sigma\psi & \sigma &\mapsto \sigma^{-1} \end{aligned}$$

son mapeos continuos pues $\varphi^{-1}(\sigma\psi N_i) \supseteq \sigma N_i \times \psi N_j$ y $i^{-1}(\sigma^{-1} N_j) = \sigma N_j$ y por lo tanto G con esta topología es un grupo topológico que además es Hausdorff ya que $\cap_{i \in I} N_i = \{e\}$.

Se tiene:

Teorema 2.2.3. *El grupo $G = \text{Gal}(L/K)$ con la topología de Krull es un grupo profinito y $G \cong \varprojlim_{i \in I} G/N_i \cong \varprojlim_{i \in I} \text{Gal}(K_i/K)$ tanto algebraica como topológicamente. En otras palabras, $\text{Gal}\left(\bigcup_i K_i/K\right) = \varprojlim_i \text{Gal}(K_i/K)$.*

Demostración. [70, Theorem 11.4.5, página 402]. □

Con esta topología tenemos:

Teorema 2.2.4 (Teorema Fundamental de la Teoría de Galois). *Sea K/F una extensión de Galois con grupo $G = \text{Gal}(K/F)$. Sean*

$$\begin{aligned} \mathcal{F}(K/F) &= \{L \mid L \text{ es un campo tal que } F \subseteq L \subseteq K\} \quad \text{y} \\ S(G) &= \{H \mid H \text{ es un subgrupo cerrado de } G\}. \end{aligned}$$

Sean

$$\Phi: \mathcal{F}(K/F) \longrightarrow S(G) \quad \text{y} \quad \Psi: S(G) \longrightarrow \mathcal{F}(K/F)$$

dadas por:

$$\begin{aligned} \Phi(L) &:= \{\sigma \in G \mid \sigma|_L = \text{Id}_L\} = \text{Gal}(K/L), \\ \Psi(H) &:= \{\alpha \in K \mid \sigma\alpha = \alpha \ \forall \sigma \in H\} = K^H. \end{aligned}$$

Entonces Φ y Ψ son biyecciones mutuamente inversas. Más aún, $L_1 \subseteq L_2$ si y solamente si $\text{Gal}(K/L_1) \supseteq \text{Gal}(K/L_2)$ y $H_1 \subseteq H_2$ si y solamente si $K^{H_1} \supseteq K^{H_2}$.

Si $\sigma \in G$ y $L \in \mathcal{F}(K/F)$, entonces

$$\text{Gal}(K/\sigma L) = \sigma \text{Gal}(K/L) \sigma^{-1}$$

y en particular $L \in \mathcal{F}(K/F)$ es una extensión normal si y solamente si $\text{Gal}(K/L)$ es normal en G y en este caso

$$\text{Gal}(L/F) \cong \frac{\text{Gal}(K/F)}{\text{Gal}(K/L)}.$$

Finalmente, los subgrupos abiertos de G corresponden a subextensiones finitas de K/F .

Demostración. [70, Theorem 11.4.9, página 405]. □

Se tiene que si G es un grupo de Galois, entonces G necesariamente G es un grupo profinito. El recíproco también se cumple.

Teorema 2.2.5 (Leptin). *Sea G un grupo profinito cualquiera. Entonces existe una extensión de campos K/F tal que $G \cong \text{Gal}(K/F)$ tanto algebraica como topológicamente donde $\text{Gal}(K/F)$ tiene la topología de Krull.*

Demostración. [70, Theorem 11.4.10, página 407]. □

Campos ciclotómicos

3.1. La función exponencial y el número π

La función exponencial $\exp(z)$ ha jugado un papel central en diversas áreas de las Matemáticas y de otras disciplinas: Ingeniería, Física, etc. La Teoría de Números y en particular, la Teoría de Campos de Clase no es la excepción. Por esto damos un muy breve repaso a las propiedades básicas de esta función.

Definición 3.1.1. La *función exponencial* $\exp: \mathbb{C} \rightarrow \mathbb{C}$ se define por $\exp(z) = e^z := \sum_{n=0}^{\infty} \frac{z^n}{n!}$.

Es un ejercicio elemental probar que la serie converge absoluta y uniformemente por compactos en \mathbb{C} . En particular $f(z) := e^z$ es una función holomorfa en \mathbb{C} y se tiene

$$f'(z) = \sum_{n=0}^{\infty} \frac{nz^{n-1}}{n!} = \sum_{n=1}^{\infty} \frac{z^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} \frac{z^n}{n!} = e^z = f(z).$$

Usando el producto de Cauchy para series y el Binomio de Newton, se tiene que para todo $z, w \in \mathbb{C}$,

$$\begin{aligned} e^z \cdot e^w &= \sum_{n=0}^{\infty} \frac{z^n}{n!} \cdot \sum_{n=0}^{\infty} \frac{w^n}{n!} = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n \frac{z^k w^{n-k}}{k!(n-k)!} \right) = \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \left(\sum_{k=0}^n \binom{n}{k} z^k w^{n-k} \right) = \sum_{n=0}^{\infty} \frac{(z+w)^n}{n!} = e^{z+w}. \end{aligned} \quad (3.1)$$

Definición 3.1.2. Se definen las funciones *seno* y *coseno*: $\text{sen}: \mathbb{C} \rightarrow \mathbb{C}$, $\text{cos}: \mathbb{C} \rightarrow \mathbb{C}$ como

$$\text{sen}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{(2n+1)!}, \quad \text{cos}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n}}{(2n)!}. \quad (3.2)$$

Es fácil verificar las siguientes propiedades para cualesquiera $z, w \in \mathbb{C}$:

- Lema 3.1.3.** (a) $e^{iz} = \cos z + i \sin z$,
 (b) $\cos^2 z + \sin^2 z = 1$,
 (c) $\sin(z + w) = \sin z \cos w + \cos z \sin w$,
 (d) $\cos(z + w) = \cos z \cos w - \sin z \sin w$,
 (e) $\cos z = \frac{e^{iz} + e^{-iz}}{2}$, $\sin z = \frac{e^{iz} - e^{-iz}}{2i}$. □

En particular, si $y \in \mathbb{R}$, entonces $\cos^2 y + \sin^2 y = 1$ y por tanto $|\cos y| \leq 1$, $|\sin y| \leq 1$ para $y \in \mathbb{R}$.

De esta forma tenemos la expresión debida a Euler: Para $z = x + iy \in \mathbb{C}$:

$$e^z = e^{x+iy} = e^x e^{iy} = e^x (\cos y + i \sin y).$$

Además, $e^z e^{-z} = e^{z-z} = e^0 = 1$ lo cual en particular implica que $e^z \neq 0$ para toda $z \in \mathbb{C}$. Por otro lado, para $x \in \mathbb{R}$, $e^x = e^{x/2+x/2} = (e^{x/2})^2 > 0$.

También se tiene que $|e^z| = |e^x| |e^{iy}| = e^x \sqrt{\cos^2 y + \sin^2 y} = e^x$ y $(\sin z)' = \cos z$, $(\cos z)' = -\sin z$. Para $y \in \mathbb{R}$,

$$\begin{aligned} \sin y &= \sum_{n=0}^{\infty} \frac{(-1)^n y^{2n+1}}{(2n+1)!} = \sum_{m=0}^{\infty} \left(\frac{(-1)^{2m} y^{4m+1}}{(4m+1)!} + \frac{(-1)^{2m+1} y^{4m+2}}{(4m+3)!} \right) \\ &= \sum_{m=0}^{\infty} \frac{y^{4m+1}}{(4m+3)!} ((4m+3)(4m+2) - y^2). \end{aligned}$$

En particular, para $0 < \sqrt{y} < \sqrt{6}$ se tiene que $\sin y > 0$ y $\cos y$ es una función decreciente en el intervalo $(0, \sqrt{6})$. Puesto que $\cos 0 = 1 > 0$ y $\cos 2 < 0$, existe un único $\xi_0 \in (0, 2)$ tal que $\cos \xi_0 = 0$.

Definición 3.1.4. Se define el número π como el único elemento $\pi \in (0, 4)$ tal que $\cos \pi/2 = 0$.

Notemos que $\sin^2 \pi/2 = 1$ y $0 < \pi/2 < \sqrt{6}$, por lo que $\sin \pi/2 > 0$ de donde se sigue que $\sin \pi/2 = 1$. Del Lema 3.1.3 es fácil verificar que $\sin \pi = 0$, $\cos 3\pi/2 = 0$ y que $\sin(z + 2\pi) = \sin z$, $\cos(z + 2\pi) = \cos z$ para toda $z \in \mathbb{C}$. En particular \sin y \cos son funciones periódicas. Sea $t_0 \in \mathbb{R}$, $t_0 > 0$ mínimo tal que $\sin(y + t_0) = \sin y$ para toda $y \in \mathbb{R}$. Se tiene que $0 < t_0 < 2\pi$.

Sea $n \in \mathbb{N}$ tal que $nt_0 \leq 2\pi < (n+1)t_0$. Entonces se tiene $t_0 = (n+1)t_0 - nt_0 > 2\pi - nt_0$ y puesto que $\sin(z + (2\pi - nt_0)) = \sin z$, y $2\pi - nt_0 < t_0$, se sigue que $2\pi = nt_0$. Ahora bien, $\sin y > 0 = \sin 0$ para $y \in (0, \pi/2]$ lo cual implica que $t_0 > \pi/2$ y en particular $2\pi = nt_0 > n\pi/2$, esto es, $n < 4$. Se tiene que $n \neq 2$ pues si $2\pi/2 = \pi$ satisface $\cos \pi = -1 \neq 1 = \cos 0$. Similarmente $n \neq 3$ pues $2\pi/3$ satisface $\sin(2\pi/3) \neq 0 = \sin 0$. Se sigue que $n = 1$, esto es, $t_0 = 2\pi$.

Similarmente para la función coseno.

Teorema 3.1.5. *El mínimo período para las funciones seno y coseno es $t_0 = 2\pi$.* \square

Corolario 3.1.6. *Se tiene $e^z = 1 \iff z = 2n\pi i, n \in \mathbb{Z}$.*

Demostración.

\Leftarrow) $e^{2n\pi i} = \cos 2n\pi + i \sin 2n\pi = \cos 0 + i \sin 0 = 1$.

\Rightarrow) Si $e^z = \cos z + i \sin z = 1$, entonces $|e^z| = e^x = 1$ esto es $x = 0$ pues e^x es una función creciente y $e^0 = 1$. Por lo tanto $z = iy, y \in \mathbb{R}$. Tenemos entonces que $\cos y + i \sin y = 1$ de donde $\cos y = 1$ y $\sin y = 0$. Por la discusión anterior, $\cos 0 = \cos y = 1$ y $\sin 0 = \sin y = 0$ de donde se sigue el resultado. \square

El desarrollo anterior nos conduce a nuestra área de interés, esto es, el cálculo de las raíces n -ésimas de la unidad, $n \in \mathbb{N}$. Más generalmente, tenemos:

Proposición 3.1.7 (Fórmula de Moivre). *Sea $z_0 \in \mathbb{C}, z_0 \neq 0$. Entonces z_0 se puede escribir como $z_0 = \rho e^{i\alpha}$, $\alpha \in \mathbb{R}, \rho \in \mathbb{R}, \rho = |z_0| > 0$. Además, para $n \in \mathbb{N}$, existen exactamente n números complejos $\omega_k, k = 0, 1, \dots, n-1$ tales que $\omega_k^n = z_0$. Los elementos ω_k están dados por*

$$\omega_k = \rho^{1/n} e^{((\alpha+2n\pi)/k)i}, k = 0, 1, \dots, n-1.$$

Demostración. Notemos que la función $g: \mathbb{R} \rightarrow S^1, g(y) := e^{iy}$ donde $S^1 = \{\xi \in \mathbb{C} \mid |\xi| = 1\}$, es suprayectiva. Además $g: [0, 2\pi) \rightarrow S^1$ es una función biyectiva. Todo lo anterior es consecuencia de la discusión anterior sobre las funciones seno y coseno y no presentamos los detalles. Por tanto, dado $z_0 \in \mathbb{C}, z_0 \neq 0$, entonces $z_1 = \frac{z_0}{|z_0|}$ satisface que $|z_1| = 1$ y por tanto existe un único $\alpha \in [0, 2\pi)$ tal que $e^{i\alpha} = z_1$. Por tanto $z_0 = \rho e^{i\alpha}, \rho = |z_0|$.

Sea $\omega \in \mathbb{C}$ tal que $\omega^n = z_0$. Escribamos $\omega = \mu e^{i\beta}, \mu = |\omega| > 0, \beta \in \mathbb{R}$. Entonces $\omega^n = \mu^n e^{in\beta} = \rho e^{i\alpha} = z_0$. Por lo tanto $\mu^n = |\omega^n| = |z_0| = \rho$, esto es, $\mu = \rho^{1/n}$. Además $e^{in\beta} = e^{i\alpha}$ lo cual equivale a $e^{i(n\beta-\alpha)} = 1$.

Por el Corolario 3.1.6 se tiene que $n\beta - \alpha = 2m\pi$ para algún $m \in \mathbb{Z}$. Se sigue que $\beta = \frac{\alpha+2m\pi}{n}$. Sea $\omega_m := \rho^{1/n} e^{((\alpha+2m\pi)/n)i}, m \in \mathbb{Z}$. Es inmediato que $\omega_m^n = z_0$ y que $\omega_m = \omega_{m'} \iff m \equiv m' \pmod{n}$. Por lo tanto hay exactamente n raíces: $\omega_0, \dots, \omega_{n-1}$. \square

Definición 3.1.8. Se define ζ_n por $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$.

Notemos que $\zeta_n^n = 1$ y que $\zeta_n^m \neq 1$ para $1 \leq m \leq n-1$. Además $\{\zeta_0^n = 1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1} = \zeta_n^{-1}\} = W_n$ son las raíces del polinomio $p(z) = z^n - 1 \in \mathbb{C}[z]$. Notemos que W_n es un grupo cíclico de orden n . Los generadores de W_n son los elementos ζ_n^a con $(a, n) = 1$.

Observación 3.1.9. Si $n|m$ entonces $\zeta_m^n = \exp\left(\frac{2\pi i}{m} \cdot n\right) = \exp\left(\frac{2\pi i}{m/n}\right) = \zeta_{m/n}$ y más generalmente, si $n = xt$ con $t|m$, $\zeta_m^n = \zeta_m^{xt} = \zeta_{m/t}^x$.

3.2. Campos Ciclotómicos

Definición 3.2.1. Para $n \in \mathbb{N}$ se define el n -ésimo campo ciclotómico por $\mathbb{Q}(\zeta_n)$.

Notemos que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois pues al ser \mathbb{Q} de característica 0, la extensión es separable y $\mathbb{Q}(\zeta_n)$ es el campo de descomposición del polinomio $x^n - 1$ sobre \mathbb{Q} . Sea $G_n := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Entonces $\sigma \in G_n$, σ está determinado por su acción en ζ_n y $\sigma\zeta_n$ debe ser una raíz de $x^n - 1$, por lo tanto $\sigma\zeta_n = \zeta_n^a$. Denotamos a este elemento por $\sigma = \sigma_a$. Ahora bien, si $\sigma^{-1}\zeta_n = \zeta_n^b$, se tiene $\zeta_n = \sigma^{-1}\sigma\zeta_n = \zeta_n^{ab}$, esto es $ab \equiv 1 \pmod{n}$ y en particular $a \in U_n = \{t \in \mathbb{Z}/n\mathbb{Z} \mid (t, n) = 1\}$ donde $t \in \mathbb{Z}$, $\bar{t} = t \pmod{n}$. Es claro que la función $\varphi: G_n \rightarrow U_n$, $\varphi(\sigma_a) = a$ es un monomorfismo de grupos. En particular G_n es un grupo abeliano.

Definición 3.2.2. Para $n \in \mathbb{N}$ se define el n -ésimo polinomio ciclotómico por

$$\psi_n(x) = \prod_{\substack{(i,n)=1 \\ 0 \leq i < n}} (x - \zeta_n^i).$$

Se tiene que $\text{gr } \psi_n(x) = |U_n| = |\{a \in \mathbb{Z} \mid 0 \leq a < n, (a, n) = 1\}| = \varphi(n)$ donde φ es la función φ de Euler.

Proposición 3.2.3. Para $n \in \mathbb{N}$ se tiene

$$x^n - 1 = \prod_{d|n} \psi_d(x).$$

Demostración. Se tiene $x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$, de donde se sigue que $\psi_d(x) | x^n - 1$ para toda $d|n$ pues $\psi_d(x) = \prod_{(i,d)=1} (x - \zeta_d^i) = \prod_{(i,d)=1} (x - \zeta_n^{in/d})$, esto es, $\zeta_n^{in/d} = \zeta_d^i$.

Ahora bien, veamos que si $d_1|n$, $d_2|n$ y $d_1 \neq d_2$ entonces $\text{mcd}(\psi_{d_1}, \psi_{d_2}) = 1$. En efecto, si δ fuese una raíz común de ψ_{d_1} y ψ_{d_2} , entonces $\delta = \zeta_{d_1}^{i_1} = \zeta_{d_2}^{i_2}$ para algunos i_1, i_2 tales que $(i_j, d_j) = 1$ para $j = 1, 2$. Entonces $\delta = \zeta_{d_1 d_2}^{i_1 d_2} = \zeta_{d_1 d_2}^{i_2 d_1}$ de donde se seguiría que $i_1 d_2 = i_2 d_1$. Puesto que $(i_1, d_1) = 1$, se tiene que $i_1 | i_2$ y viceversa por lo que $i_1 = i_2$ y $d_1 = d_2$ contrario a lo supuesto. Por lo tanto

$$\prod_{d|n} \psi_d(x) | x^n - 1.$$

La igualdad se sigue de que ambos polinomios son mónicos y de que

$$\text{gr}\left(\prod_{d|n} \psi_d(x)\right) = \sum_{d|n} \varphi(d) = n = \text{gr}(x^n - 1). \quad \square$$

La igualdad $\sum_{d|n} \varphi(d) = n$ la probamos a continuación.

Proposición 3.2.4. Sea $n \in \mathbb{N}$ y sea φ la función fi de Euler. Entonces $\sum_{d|n} \varphi(d) = n$.

Demostración. Damos dos demostraciones. Para la primera, consideremos C_n un grupo cíclico de n elementos. Sea $A_t := \{x \in C_n \mid o(x) = t\}$ donde $o(x)$ denota el orden del elemento x . Si $t \nmid n$, se tiene que $A_t = \emptyset$. Si $t \mid n$, entonces C_n tiene un único subgrupo H_t de orden t y puesto que C_n es cíclico, este subgrupo es a su vez cíclico. Los elementos de orden t de C_n son precisamente los generadores de H_t y por tanto $|A_t| = \varphi(t)$.

Se tiene que si $d_1 \neq d_2$, $A_{d_1} \cap A_{d_2} = \emptyset$ y cada $x \in C_n$ está en algún A_t , de donde:

$$n = |C_n| = \sum_{t=1}^n |A_t| = \sum_{t|n} |A_t| = \sum_{t|n} \varphi(t).$$

Esto termina la primera demostración.

Presentamos una segunda demostración más directa. Primero, si p es un número primo y $\alpha \in \mathbb{N}$, entonces $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Por tanto

$$p^\alpha = \sum_{t=1}^{\alpha} (p^t - p^{t-1}) + 1 = \sum_{t=1}^{\alpha} \varphi(p^t) + 1 = \sum_{t=0}^{\alpha} \varphi(p^t),$$

En general, puesto que φ es una función multiplicativa, es decir, si $\text{mcd}(n, m) = 1$, $\varphi(nm) = \varphi(n)\varphi(m)$, se tiene en general que si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con p_1, \dots, p_r primos distintos y $\alpha_i \geq 1$, $1 \leq i \leq r$, entonces

$$\begin{aligned} n &= p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i} = \prod_{i=1}^r \left(\sum_{j_i=1}^{\alpha_i} \varphi(p_i^{j_i}) \right) = \sum_{0 \leq j_i \leq \alpha_i} \prod_{i=1}^r \varphi(p_i^{j_i}) \\ &= \sum_{0 \leq j_i \leq \alpha_i} \varphi\left(\prod_{i=1}^r p_i^{j_i}\right) = \sum_{\substack{0 \leq \beta_i \leq \alpha_i \\ 0 \leq i \leq r}} \varphi(p_1^{\beta_1} \cdots p_r^{\beta_r}) = \sum_{d|n} \varphi(d). \end{aligned}$$

Esto termina la segunda demostración. \square

Ahora bien como consecuencia de la Proposición 3.2.3 tenemos:

Corolario 3.2.5. $\psi_n(x) \in \mathbb{Z}[x]$ para toda $n \in \mathbb{N}$.

Demostración. Lo hacemos por inducción en n . Para $n = 1$, se tiene que $\psi_1(x) = x - 1 \in \mathbb{Z}[x]$. Sea $n > 1$ y suponemos que $\psi_d(x) \in \mathbb{Z}[x]$ para toda $d < n$. Entonces $x^n - 1 = \prod_{d|n} \psi_d(x) = \psi_n(x) \cdot \prod_{\substack{d|n \\ d < n}} \psi_d(x)$.

Ahora $\prod_{\substack{d|n \\ d < n}} \psi_d(x) = h(x) \in \mathbb{Z}[x]$. Por lo tanto $\psi_n(x) = \frac{x^n - 1}{h(x)} \in \mathbb{Q}[x]$ de donde $x^n - 1 = h(x)\psi_n(x)$. Ahora bien, usando ya sea el Lema de Gauss o el algoritmo de la división para dominios enteros y que $h(x)$ es un polinomio mónico, se sigue que $\psi_n(x) \in \mathbb{Z}[x]$. \square

Ejemplos 3.2.6.

- (1) $\psi_1(x) = x - 1$,
 $\psi_2(x) = x + 1 = \frac{x^2-1}{x-1}$,
 $\psi_3(x) = x^2 + x + 1 = \frac{x^3-1}{x-1}$,
 $\psi_4(x) = x^2 + 1 = \frac{x^4-1}{\psi_1(x)\psi_2(x)} = \frac{x^4-1}{x^2-1}$,
 $\psi_5(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$.
(2) Si p es un número primo,

$$\psi_p(x) = \frac{x^p - 1}{\psi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

- (3) Si p es un número primo entonces

$$\begin{aligned} \psi_{p^n}(x) &= \frac{x^{p^n} - 1}{\prod_{i=0}^{n-1} \psi_{p^i}(x)} = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} \\ &= x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1 = \psi_p(x^{p^{n-1}}). \end{aligned}$$

En particular $\psi_{p^n}(1) = \underbrace{1 + 1 + \cdots + 1}_{p \text{ veces}} = p$ y

$$p = \prod_{\substack{i=0 \\ (i,p)=1}}^{p^n-1} (1 - \zeta_{p^n}^i).$$

Notemos además que por el criterio de Eisenstein, $\psi_p(x) \in \mathbb{Z}[x]$ es irreducible. Esto no es casualidad como veremos a continuación.

Proposición 3.2.7. *Si n y m son primos relativos, entonces $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$. En consecuencia si la descomposición en primos de n está dado por $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ entonces $\mathbb{Q}(\zeta_n) = \prod_{i=1}^r \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$.*

Demostración. Se tiene $\zeta_n = \zeta_{nm}^m$ y $\zeta_m = \zeta_{nm}^n$ por tanto $\mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$ (de hecho esto se cumple para todas $n, m \in \mathbb{N}$).

Ahora, sean $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha n + \beta m = 1$. Por tanto

$$\zeta_{nm} = \zeta_{nm}^{\alpha n + \beta m} = \zeta_{nm}^{\alpha n} \zeta_{nm}^{\beta m} = \zeta_m^{\alpha} \zeta_n^{\beta} \in \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m).$$

Por tanto $\mathbb{Q}(\zeta_{nm}) \subseteq \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$ de donde se sigue la igualdad. \square

Teorema 3.2.8. *Para cualquier $n \in \mathbb{N}$, $\psi_n(x) \in \mathbb{Z}[x]$ es irreducible sobre \mathbb{Q} .*

Demostración. Sea $f(x) := \text{Irr}(\zeta_n, x, \mathbb{Q})$ el polinomio irreducible de ζ_n sobre \mathbb{Q} . Puesto que $\psi_n(\zeta_n) = 0$, se tiene que $f(x) | x^n - 1$. Ahora bien, sea $x^n - 1 = f(x)g(x)$ con $f(x)$ y $g(x)$ con coeficiente líder igual a 1. Por el Lema de

Gauss se sigue que $f(x), g(x) \in \mathbb{Z}[x]$. Notemos que las raíces de $\psi_n(x)$ son $\{\zeta_n^d\}_{(d,n)=1}$. En particular cualquier raíz de $\psi_n(x)$ es de la forma $\zeta_n^{p_1 \cdots p_r}$ con p_1, \dots, p_r números primos, no necesariamente distintos, tales que $p_i \nmid n$. Ahora bien, si probamos que dada cualquier raíz λ de $f(x)$, entonces λ^p , con p un número primo tal que $p \nmid n$, es raíz de $f(x)$, entonces se tendrá que toda raíz de $\psi_n(x)$ será también raíz de $f(x)$ y en particular se seguirá que $\psi_n(x) | f(x)$ de donde se obtendrá la igualdad $\psi_n(x) = f(x)$ y que $\psi_n(x)$ es irreducible.

En resumen, vamos a probar que si λ es cualquier raíz de $f(x)$, entonces λ^p es también de $f(x)$ con p es un número primo tal que $p \nmid n$.

Supongamos que λ es raíz de $f(x)$ pero que λ^p no lo es. Puesto que λ^p es raíz de $x^n - 1$, entonces $g(\lambda^p) = 0$. Puesto que $f(\lambda) = 0$ y $f(x)$ es irreducible y λ es raíz de $g(x^p)$, se sigue que $f(x) | g(x^p)$. Pongamos $g(x^p) = f(x)h(x)$ con $h(x) \in \mathbb{Z}[x]$ por el Lema de Gauss.

Por otro lado, si $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \in \mathbb{Z}[x]$, entonces

$$\begin{aligned} g(x)^p &\equiv (x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0)^p \pmod{p} \\ &\equiv x^{pm} + b_{m-1}^p x^{p(m-1)} + \cdots + b_1^p x^p + b_0^p \pmod{p} \\ &\equiv (x^p)^m + b_{m-1}(x^p)^{m-1} + \cdots + b_1(x^p) + b_0 \pmod{p} \equiv g(x^p) \pmod{p}. \end{aligned}$$

Esto es, módulo p , $g(x)^p \equiv f(x)h(x) \pmod{p}$. En particular $\overline{g(x)} := g(x) \pmod{p} \in \mathbb{F}_p[x]$ y $\overline{f(x)}$ no son primos relativos en $\mathbb{F}_p[x]$ y puesto que $\overline{x^n - 1} = \overline{f(x)g(x)}$, se tiene que $\overline{x^n - 1} \in \mathbb{F}_p[x]$ tiene raíces múltiples. Sin embargo la derivada de $\overline{x^n - 1}$ es $\overline{nx^{n-1}} \not\equiv 0 \pmod{p}$ pues $p \nmid n$. La única raíz de la derivada de $\overline{x^n - 1}$ es $\bar{0}$ la cual no es raíz de $\overline{x^n - 1}$ de donde se sigue que $\overline{x^n - 1}$ no tiene raíces múltiples. Esta contradicción prueba que λ^p es raíz de $f(x)$ y termina la demostración del teorema. \square

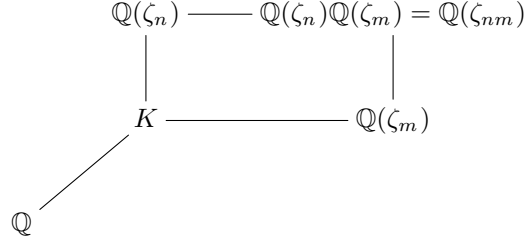
Observación 3.2.9. Se podría dar otra demostración de que $\psi_n(x)$ es irreducible probando que si p es un número primo y $m \in \mathbb{N}$, entonces $\psi_{p^m}(x)$ es irreducible por medio del cálculo del índice de ramificación de p en $\mathbb{Q}(\zeta_{p^m})$ probando que $e \geq \varphi(p^m)$. De esta forma, y viendo que no hay más ramificación, se seguiría que si $\text{mcd}(m, n) = 1$, $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ y en consecuencia, usando que la función φ de Euler es multiplicativa se deduciría que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ y que $\psi_n(x)$ es irreducible. Claramente esta demostración es mucho más complicada que la presentada, sin embargo basta hallar una demostración independiente de que $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ para n, m primos relativos.

Corolario 3.2.10. Para $n \in \mathbb{N}$, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \text{gr } \psi_n(x)$ y $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois con grupo de Galois isomorfo a $U_n := (\mathbb{Z}/n\mathbb{Z})^*$.

Demostración. Se tiene $G_n = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \subseteq U_n$ y $|G_n| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \text{gr } \psi_n = |U_n|$ de donde se sigue que son iguales. \square

Corolario 3.2.11. *Si m y n son primos relativos, entonces $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. En particular $\text{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.*

Demostración. Sea $K := \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$. Se tiene el diagrama



Entonces

$$\begin{aligned}
 \varphi(nm) = \varphi(n)\varphi(m) &= [\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] \\
 &= [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m) : \mathbb{Q}].
 \end{aligned}$$

Es decir

$$\varphi(n)\varphi(m) = [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_n)]\varphi(n) = [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_m)]\varphi(m).$$

Se sigue que $\varphi(m) = [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_n)]$ y $\varphi(n) = [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_m)]$. En particular tenemos

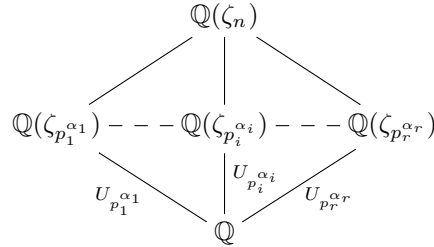
$$\begin{aligned}
 \varphi(n) &= [\mathbb{Q}(\zeta_{nm})\mathbb{Q}(\zeta_m)] \leq [\mathbb{Q}(\zeta_n) : K] \\
 &\leq [\mathbb{Q}(\zeta_n) : K][K : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)
 \end{aligned}$$

lo cual implica que $[\mathbb{Q}(\zeta_n) : K] = \varphi(n)$ y por lo tanto $K = \mathbb{Q}$. La igualdad $\text{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ se sigue de la Teoría de Galois. \square

El siguiente resultado es una consecuencia inmediata del Teorema Chino del Residuo. Aquí presentamos otra demostración usando los resultados hasta ahora obtenidos en campos ciclotómicos.

Corolario 3.2.12. *Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con p_1, \dots, p_r primos distintos, entonces $U_n \cong U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}$.*

Demostración. Se tiene el diagrama



Por lo tanto

$$U_n \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_{i=1}^r \text{Gal}(\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}) \cong \prod_{i=1}^r U_{p_i^{\alpha_i}}. \quad \square$$

Como hicimos notar antes, se tiene que si p es un número primo y $n \in \mathbb{N}$, entonces $\psi_{p^n}(x) = \psi_p(x^{p^{n-1}})$ (Ejemplo 3.2.6 (3)). Más generalmente, tenemos

Proposición 3.2.13. *Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la descomposición en primos, entonces $\psi_n(x) = \psi_{p_1 \cdots p_r}(x^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}})$.*

Demostración. Primero notemos que

$$\begin{aligned} \text{gr}(\psi_{p_1 \cdots p_r}(x^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}})) &= x^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}} \text{gr} \psi_{p_1 \cdots p_r}(x) \\ &= p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1} \varphi(p_1 \cdots p_r) = \varphi(n) = \text{gr} \psi_n(x). \end{aligned}$$

Ahora $\zeta_n^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}} = \zeta_{p_1 \cdots p_r}$ lo cual implica que ζ_n es raíz del polinomio $\psi_{p_1 \cdots p_r}(x^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}})$ de donde $\psi_n(x) | \psi_{p_1 \cdots p_r}(x^{p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1}})$ lo cual implica que ambos son iguales. \square

Recordemos la fórmula de inversión de Möbius. Consideremos las funciones $\mu: \mathbb{N} \rightarrow \mathbb{Q}$, $\varepsilon: \mathbb{N} \rightarrow \mathbb{Q}$ dadas por

$$\begin{aligned} \mu(n) &= \begin{cases} 1 & \text{si } n = 1; \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ con } p_1, \dots, p_r \text{ son primos distintos;} \\ 0 & \text{en otro caso, esto es, si existe } d > 1, d^2 | n. \end{cases} \\ \varepsilon(n) &= \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } n > 1. \end{cases} \end{aligned}$$

Entonces se tiene

Lema 3.2.14. $\sum_{d|n} \mu(d) = \varepsilon(n)$.

Demostración. Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la descomposición en primos de n . Entonces

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{i_1 < \cdots < i_t} \mu(p_{i_1} \cdots p_{i_t}) = \sum_{t=0}^r \binom{r}{t} (-1)^t = (1-1)^r = 0^r \\ &= \begin{cases} 1 & \text{si } r = 0 \\ 0 & \text{si } r > 0 \end{cases} = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases} = \varepsilon(n). \quad \square \end{aligned}$$

Corolario 3.2.15 (Fórmula de Inversión de Möbius). *Sea k cualquier campo y sean $f, g: \mathbb{N} \rightarrow k$ dos funciones tales que:*

(1) $f(n) = \sum_{d|n} g(d)$. Entonces

$$g(n) = \sum_{d|n} \mu(n/d) f(d) = \sum_{d|n} \mu(d) f(n/d).$$

(2) Si $f(n), g(n) \neq 0$ para toda $n \in \mathbb{N}$ y $f(n) = \prod_{d|n} g(d)$. Entonces

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)} = \prod_{d|n} f(n/d)^{\mu(d)}.$$

Demostración.

(1) Se tiene que $\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) (\sum_{s|\frac{n}{d}} g(s))$. Ahora bien, si $s|\frac{n}{d}$, entonces $d|\frac{n}{s}$. Por tanto, la última suma es del tipo $\sum_{t|n} a_t g(t)$ para algunos $a_t \in \mathbb{Z}$.

Obtenemos $a_t = \sum_{d|\frac{n}{t}} \mu(d) = \varepsilon(n/t) = \begin{cases} 1 & \text{si } n = t \\ 0 & \text{si } n \neq t \end{cases}$. Por lo tanto, por el Lema 3.2.14 se tiene

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{t|n} a_t g(t) = g(n).$$

(2) Tenemos

$$\prod_{d|n} f(d)^{\mu(n/d)} = \prod_{d|n} \left[\prod_{t|d} g(t) \right]^{\mu(n/d)} = \prod_{a|t} g(a)^{s(a)}$$

donde

$$s(a) = \sum_{a|d} \mu(n/d) = \sum_{t|\frac{n}{a}} \mu(t) = \varepsilon(n/a)$$

de donde se sigue el resultado. \square

La fórmula de inversión de Möbius nos da una expresión para el polinomio ciclotómico en términos de los polinomios $x^n - 1$.

Proposición 3.2.16. Para $n \in \mathbb{N}$ se tiene

$$\psi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Demostración. Sean $f, g: \mathbb{N} \rightarrow \mathbb{Q}(x)$, donde $\mathbb{Q}(x)$ es el campo de las funciones racionales sobre \mathbb{Q} dadas por

$$f(n) := x^n - 1, \quad g(m) := \psi_m(x).$$

Por la Proposición 3.2.3 se tiene que $f(n) = \prod_{d|n} g(d)$. Del Corolario 3.2.15 se sigue que $g(n) = \prod_{d|n} f(d)^{\mu(n/d)}$ que es el resultado enunciado. \square

Ejemplo 3.2.17. Se tiene

$$\begin{aligned}
 \psi_{12}(x) &= \prod_{d|12} (x^d - 1)^{\mu(12/d)} \stackrel{\uparrow}{=} \prod_{d \in \{1, 2, 3, 4, 6, 12\}} (x^d - 1)^{\mu(12/d)} \\
 &= (x - 1)^{\mu(12)} (x^2 - 1)^{\mu(6)} (x^3 - 1)^{\mu(4)} \\
 &\quad (x^4 - 1)^{\mu(3)} (x^6 - 1)^{\mu(2)} (x^{12} - 1)^{\mu(1)} \\
 &= (x - 1)^0 (x^2 - 1)^1 (x^3 - 1)^0 (x^4 - 1)^{-1} (x^6 - 1)^{-1} (x^{12} - 1) \\
 &= \frac{x^{12} - 1}{x^6 - 1} \cdot \frac{1}{\left(\frac{x^4 - 1}{x^2 - 1}\right)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1.
 \end{aligned}$$

Por lo tanto $\psi_{12}(x) = x^4 - x^2 + 1$.

Observación 3.2.18. Si n es impar, entonces $\varphi(2n) = \varphi(n)$ y $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{2n})$ de donde se sigue que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$. Por lo tanto, siempre que consideremos un campo ciclotómico $\mathbb{Q}(\zeta_m)$, supondremos que $m \not\equiv 2 \pmod{4}$.

3.2.1. Estructura de U_n

Puesto que $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U_n$ es importante determinar la estructura de este último grupo.

Definición 3.2.19. Sea $p \in \mathbb{N}$ un número primo. Entonces definimos la *valuación p -ádica* v_p de \mathbb{Q}^* por $v_p: \mathbb{Q}^* \rightarrow \mathbb{Z}$ dada de la siguiente forma. Para $a \in \mathbb{Z}$, podemos escribir $a = \pm p^n b$ con $n \geq 0$, $b \in \mathbb{N}$. Entonces $v_p(a) := n$.

Si $\alpha = \frac{a}{b} \in \mathbb{Q}^*$, $a, b \in \mathbb{Z} \setminus \{0\}$, se define

$$v_p(\alpha) := v_p(a) - v_p(b).$$

Notemos que si $x, y \in \mathbb{Z} \setminus \{0\}$, entonces $v_p(xy) = v_p(x) + v_p(y)$ por lo tanto si $\alpha = \frac{a}{b} = \frac{c}{d} \in \mathbb{Q}^*$, entonces $ad = bc$ y $v_p(ad) = v_p(a) + v_p(d) = v_p(b) + v_p(c) = v_p(bc)$ de donde se sigue que $v_p(a) - v_p(b) = v_p(c) - v_p(d)$ y por lo tanto la definición de $v_p(\alpha)$ no depende de la representación de α como cociente de dos enteros.

De la misma forma, se sigue que si $\alpha, \beta \in \mathbb{Q}^*$, entonces $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$; $v_p(\alpha^{-1}) = -v_p(\alpha)$ y $v_p\left(\frac{\alpha}{\beta}\right) = v_p(\alpha) - v_p(\beta)$. Más aún $\alpha = \frac{a}{b}$ puede escribirse de manera única como $\alpha = p^m \frac{c}{d}$ con $p \nmid cd$ y $m \in \mathbb{Z}$. Entonces se tiene $v_p(\alpha) = m$.

Notemos que $v_p(-\alpha) = v_p(\alpha)$ y que $v_p(1) = 0$. Se define $v_p(0) := \infty$ donde ∞ es cualquier símbolo al que supondremos sujeto a las siguientes reglas:

1. Para toda $a \in \mathbb{Z}$, se tiene $a < \infty$;
2. $\infty + \infty = \infty \cdot \infty = \infty$;
3. Si $a \in \mathbb{Z} \setminus \{0\}$, $a \cdot \infty = \infty$;

4. El símbolo $0 \cdot \infty$ no se define.

Con esta convención se tiene:

Teorema 3.2.20. *Para $\alpha, \beta \in \mathbb{Q}$ se tiene que*

$$v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$$

y si $v_p(\alpha) \neq v_p(\beta)$ entonces

$$v_p(\alpha + \beta) = \min\{v_p(\alpha), v_p(\beta)\}.$$

Demostración. Si α o $\beta = 0$ no hay nada que probar. Sean $\alpha, \beta \neq 0$. Escribamos $\alpha = p^n \frac{c}{d}$, $\beta = p^m \frac{e}{f}$ con $p \nmid cde f$, $n, m \in \mathbb{Z}$. Entonces

$$\alpha + \beta = p^n \frac{c}{d} + p^m \frac{e}{f} = \frac{p^n c f + p^m e d}{d f} = \frac{p^r g}{d f}$$

donde $r := \min\{n, m\}$ y $g \in \mathbb{Z}$. Por lo tanto

$$v_p(\alpha + \beta) \geq r = \min\{v_p(\alpha), v_p(\beta)\}$$

lo cual prueba nuestra primera afirmación

Ahora, si $v_p(\alpha) \neq v_p(\beta)$, es decir $n \neq m$, se tiene que $p \nmid g$ y por lo tanto $v_p(\alpha + \beta) = \min\{v_p(\alpha), v_p(\beta)\}$.

Alternativamente, digamos $n < m$. Entonces $v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$ y además

$$\begin{aligned} v_p(\alpha) &= v_p(\alpha + \beta - \beta) \geq \min\{v_p(\alpha + \beta), v_p(-\beta)\} \\ &= \min\{v_p(\alpha + \beta), v_p(\beta)\} \geq v_p(\alpha). \end{aligned}$$

Por lo tanto $v_p(\alpha) = \min\{v_p(\alpha + \beta), v_p(\beta)\}$ y $v_p(\alpha) < v_p(\beta)$ lo cual implica que $v_p(\alpha) = v_p(\alpha + \beta)$. \square

Consideremos ahora el grupo U_{p^n} con p un número primo. Si $n = 1$, entonces $U_p = (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$ con \mathbb{F}_p el campo finito de p elementos. Se tiene que el grupo multiplicativo de un campo finito es cíclico. Por lo tanto $U_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Ahora supongamos que $p > 2$ y que $n \geq 1$. Entonces

$$|U_{p^n}| = \varphi(p^n) = p^{n-1}(p-1).$$

Sea $x := 1 + p$. Entonces

$$x^{p^k} = (1 + p)^{p^k} = 1 + \sum_{i=1}^{p^k} \binom{p^k}{i} p^i = 1 + p^{k+1} + \sum_{i=2}^{p^k} \binom{p^k}{i} p^i.$$

Veamos que $v_p\left(\binom{p^k}{i}p^i\right) > v_p\left(\binom{p^k}{1}p\right) = p^{k+1}$ para $2 \leq i \leq p^k$. Sea

$$\begin{aligned} A &:= v_p\left(\binom{p^k}{i}p^i\right) - v_p\left(\binom{p^k}{1}p\right) = v_p\left(\frac{1}{p^k}\binom{p^k}{i}p^{i-1}\right) \\ &= v_p\left(\frac{1}{i}\binom{p^k-1}{i-1}\right) + (i-1) \geq i-1 - v_p(i). \end{aligned}$$

Se tiene que para $a \geq 1$ y p un número primo $a \leq p^a - (p-1)$ y la desigualdad es estricta para $a \geq 2$. Si $\text{mcd}(i, p) = 1$ entonces $v_p(i) = 0$ y por tanto $A \geq i-1 \geq 1 > 0$, $2 \leq i \leq p^k$. Si $i = p^a b$, $\text{mcd}(p, b) = 1$, entonces $v_p(i) = a \leq p^a b - (p-1) = i - (p-1)$, de donde $A \geq (i-1) - i + (p-1) \geq p-2 > 0$.

En resumen, si $x = 1 + p$, entonces $x^{p^k} = 1 + p^{k+1} + sp^{k+2}$ para algún $s \in \mathbb{Z}$ y en particular $x^{p^k} \equiv 1 \pmod{p^n} \iff k+1 \geq n \iff k \geq n-1$. Se sigue que el orden de $x \pmod{p^n}$ es p^{n-1} . Por otro lado tenemos el epimorfismo natural

$$\begin{aligned} U_{p^n} &\rightarrow U_p \\ \xi \pmod{p^n} &\mapsto \xi \pmod{p} \end{aligned}$$

de donde tenemos que existe $y \in U_{p^n}$ de orden $(p-1)$ y por tanto xy es de orden $p^{n-1}(p-1) = \varphi(p^n) = |U_{p^n}|$ probando que U_{p^n} es un grupo cíclico para $p > 2$, con p primo y $n \in \mathbb{N}$.

Ahora consideremos el caso 2^n . Se tiene $U_2 = \{1\}$; $U_4 = (\mathbb{Z}/4\mathbb{Z})^* \cong \{\pm 1\} \cong C_2$. Notemos que U_8 no es cíclico: $U_8 = \{1, 3, 5, 7\}$ y todos sus elementos son de orden 2: $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, es decir, $U_8 \cong C_2 \times C_2$.

Para $n \geq 3$ se tiene la sucesión exacta

$$1 \longrightarrow D_{2^n, 4} \longrightarrow U_{2^n} \xrightarrow{\varphi} U_4 \longrightarrow 1 \quad (3.3)$$

donde φ es el epimorfismo natural y $D_{2^n, 4} := \text{núc } \varphi = \{x \pmod{2^n} \mid x \equiv 1 \pmod{4}\}$.

Se tiene en particular que $5 = 1 + 2^2 \in D_{2^n, 4}$ y de manera similar como antes, es decir considerando las potencias $(1+2^2)^{2^k}$, se tiene que $o(5 \pmod{2^n}) = 2^{n-2}$ y en particular $D_{2^n, 4}$ es un grupo cíclico de orden 2^{n-2} .

Ahora, para $x \in U_{2^n}$, si $x \in D_{2^n, 4} = \langle 5 \rangle$ se tiene que $o(x) \mid 2^{n-2}$. Si $x \notin D_{2^n, 4}$ entonces $x \equiv 3 \pmod{4}$. Escribamos $x = 3 + 2^2 a$. Entonces $x^2 = 9 + 24a + 2^4 a^2 = 1 + 2^3 t$ de donde obtenemos, como en la primera parte, que $o(x^2) \mid 2^{n-3}$. De aquí se sigue que $o(x) \mid 2^{n-2}$ y que todo elemento $x \in U_{2^n}$ tiene orden menor o igual a 2^{n-2} por lo que para $n \geq 3$, U_{2^n} no es un grupo cíclico lo cual también se sigue del hecho de que existe un epimorfismo natural $U_{2^n} \rightarrow U_8$ y de que U_8 no es cíclico, pero de esta forma obtuvimos un elemento de orden exactamente 2^{n-2} .

Puesto que $|U_{2^n}| = 2^{n-1}$ se sigue que $U_{2^n} \cong C_{2^{n-2}} \times C_2$. Este isomorfismo también se sigue de que la sucesión (3.3) se escinde: sea $\psi : U_4 \rightarrow U_{2^n}$, $\psi(3) = \psi(-1) = 2^n - 1$ y $(\varphi \circ \psi)(3) = \varphi(2^n - 1) = \varphi(3 + 2^n - 4) = 3$ y en particular

$$U_{2^n} \cong D_{2^n,4} \times U_4.$$

Finalmente, para $n \in \mathbb{N}$, $n \geq 3$, se tiene que si la descomposición en primos de n es $n = 2^m p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con p_1, \dots, p_r primos impares distintos, $m \geq 0$, $\alpha_i \geq 0$, $r \geq 0$, entonces por el Teorema Chino del Residuo se tiene

$$U_n \cong U_{2^m} \times U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}.$$

Resumimos nuestra discusión anterior en el siguiente resultado.

Teorema 3.2.21. *Sea $n \geq 3$, $n = 2^m p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ en su descomposición en primos. Entonces, si $m \geq 2$*

$$U_n \cong C_2 \times C_{2^{m-2}} \times C_{p_1-1} \times \cdots \times C_{p_r-1} \times C_{p_1^{\alpha_1}} \times \cdots \times C_{p_r^{\alpha_r}}. \quad (3.4)$$

Si $m = 0, 1$, entonces

$$U_n \cong C_{p_1-1} \times \cdots \times C_{p_r-1} \times C_{p_1^{\alpha_1}} \times C_{p_r^{\alpha_r}}. \quad (3.5)$$

En particular U_n es un grupo cíclico $\iff n = 2, 4, p^\alpha, 2p^\alpha$ con p un número primo impar, $\alpha \geq 1$.

Demostración. La ciclicidad se sigue del hecho de que si p_i es impar, entonces $p_i - 1$ es par. \square

Recordemos que si $\mathbb{Q}(\zeta_n)$ es un campo ciclotómico, entonces $n \not\equiv 2 \pmod{4}$. Entonces se sigue

Corolario 3.2.22. *La extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es cíclica para $n = 4$ y para $n = p^\alpha$ con p un primo impar y $\alpha \geq 1$.* \square

Más adelante estudiaremos con más detalle la correspondencia de Galois entre los subcampos de $\mathbb{Q}(\zeta_n)$ y los subgrupos de U_n .

Recordemos que dado un campo numérico K/\mathbb{Q} , $[K : \mathbb{Q}] = n < \infty$, entonces el anillo de enteros \mathcal{O}_K de K se define por

$$\mathcal{O}_K = \{\alpha \in K \mid \text{Irr}(\alpha, x, \mathbb{Q}) \in \mathbb{Z}[x]\}.$$

Equivalentemente, \mathcal{O}_K es la cerradura entera de \mathbb{Z} en K y \mathcal{O}_K es un \mathbb{Z} -módulo libre de rango $n = [K : \mathbb{Q}]$.

Una *base entera* $\{\alpha_1, \dots, \alpha_n\}$ es una base de \mathcal{O}_K como \mathbb{Z} -módulo, es decir,

$$\mathcal{O}_K \cong \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Finalmente, el *discriminante* de K se define por

$$\delta_K := \det \left(\alpha_i^\sigma \right)_{\substack{1 \leq i \leq n \\ \sigma \in T}}^2 \in \mathbb{Z}$$

donde T es el conjunto de encajes de K en \mathbb{C} ,

$$T := \{ \sigma : K \longrightarrow \mathbb{C} \mid \sigma \text{ es monomorfismo de campos} \}.$$

Más precisamente, si $T = \{ \sigma_1, \dots, \sigma_n \}$, entonces sea

$$C = \begin{pmatrix} \alpha_1^{\sigma_1} & \cdots & \alpha_n^{\sigma_1} \\ \vdots & & \vdots \\ \alpha_1^{\sigma_n} & \cdots & \alpha_n^{\sigma_n} \end{pmatrix} \quad \text{y} \quad \delta_K = \det C^2.$$

Como de costumbre escribimos $n = r_1 + 2r_2$ donde r_1 es el número de elementos $\sigma \in T$ tales que $\sigma(K) \subset \mathbb{R}$, los cuales se llaman *encajes reales*, y $2r_2$ es el número de elementos $\sigma \in T$ tales que $\sigma(K) \not\subset \mathbb{R}$ los cuales se llaman *encajes complejos* y son un número par pues si $\sigma(T) \not\subset \mathbb{R}$ entonces $\overline{\sigma(K)} \not\subset \mathbb{R}$.

Teorema 3.2.23. *Para cualquier campo numérico, el signo del discriminante δ_K es $(-1)^{r_2}$.*

Demostración. Sea $C = (\alpha_i^{\sigma_j})_{1 \leq i, j \leq n}$ con la notación anterior. Tomando la matriz conjugada de C la cual consiste en conjugar cada elemento de C , se tiene $\det \overline{C} = \det(\overline{\alpha_i^{\sigma_j}}) = (-1)^{r_2} \det C$ pues si σ_j es real, entonces $\overline{\sigma_j(\alpha_i)} = \sigma_j(\alpha_i)$ y la fila respectiva permanece sin cambios y en el caso en que σ_j es complejo se intercambian las filas $\sigma_j(\alpha_i)$ con $\overline{\sigma_j(\alpha_i)}$ y por cada permutación de filas hay un cambio de signo. Se sigue que

$$0 < |\det C|^2 = (\det \overline{C})(\det C) = (-1)^{r_2} (\det C)^2 = (-1)^{r_2} \det C^2 = (-1)^{r_2} \delta_K. \quad \square$$

Notemos que cuando K/\mathbb{Q} es Galois, $T = \text{Gal}(K/\mathbb{Q})$ y $\sigma(K) = K$ para todo $\sigma \in T$. En particular $r_1 = 0$ si $K \not\subset \mathbb{R}$ y en cuyo caso $r_2 = \frac{n}{2}$, en donde $n = [K : \mathbb{Q}]$ o $r_2 = 0$ si $K \subseteq \mathbb{R}$ y en cuyo caso $r_1 = n$. En particular, si $K = \mathbb{Q}(\zeta_n)$, $K \subseteq \mathbb{R} \iff K = \mathbb{Q}, n = 0, 1$. Por tanto $r_1 = 0$ y $r_2 = \frac{\varphi(n)}{2}$. Si $n = 2^m p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, entonces $\varphi(n)/2$ es par excepto cuando $r = 0, m = 2$ o $r = 1, m = 0$ y $p = p_1$ es primo impar congruente con 3 módulo 4. Es decir

Proposición 3.2.24. *Si $K = \mathbb{Q}(\zeta_n)$ entonces δ_K es positivo excepto para $\mathbb{Q}(\zeta_4)$ y para $\mathbb{Q}(\zeta_{p^\alpha})$ con p número primo tal que $p \equiv 3 \pmod{4}$.* \square

La definición que hemos usado para discriminante δ_K es como un número entero. Recordemos como definimos el discriminante como un ideal. En general, consideremos un dominio Dedekind A y sea K una extensión finita y separable de $E := \text{coc } A$.

Sea B la cerradura entera de A en K : $B := \{\alpha \in K \mid \text{Irr}(\alpha, x, E) \in A[x]\}$. Entonces B es un dominio Dedekind ([38, Cap. 1, Theorem 6.1]). Esto último se cumple aún cuando K/E no sea separable. Puesto que K/E es separable, la traza $\text{Tr} = \text{Tr}_{K/E}: K \rightarrow E$ es suprayectiva. El mapeo

$$\varphi: K \times K \rightarrow E \quad \text{dado por} \quad \varphi(x, y) := \text{Tr}(xy)$$

es E -bilineal y no degenerado, esto es, si $\text{Tr}(xy) = 0$ para toda $y \in K$ entonces $x = 0$ y recíprocamente.

Se define $B^* := \{x \in K \mid \text{Tr}(xy) \in A \text{ para toda } y \in B\}$. Entonces $B \subseteq B^*$ y B^* es un B -módulo fraccionario. El inverso es un ideal de B llamado el *diferente* de B/A : $\mathfrak{D}_{K/E} = \mathfrak{D}_{B/A} := (B^*)^{-1}$ y la norma $N_{K/E}(\mathfrak{D}_{B/A})$ se llama el *discriminante* de B sobre A .

En nuestro caso, si E es un campo numérico cualquiera y K es un extensión finita de E , tomaremos $A = \mathcal{O}_E$ y se tiene $B = \mathcal{O}_K$ y $\mathfrak{D}_{\mathcal{O}_K/\mathcal{O}_E} := \mathfrak{D}_{K/E}$ es el *diferente* de K/E . Usaremos para el discriminante la siguiente notación:

$$\mathfrak{d}_{K/E} := N_{K/E}(\mathfrak{D}_{K/E}).$$

En el caso particular de $E = \mathbb{Q}$, pondremos $\mathfrak{d}_K := \mathfrak{d}_{K/\mathbb{Q}}$ y $\mathfrak{d}_K = \langle \delta_k \rangle$.

En general, cuando tenemos un campo numérico K y $K = \mathbb{Q}(\alpha)$ con $\alpha \in \mathcal{O}_K$, entonces $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una base de K/\mathbb{Q} donde $n = [K : \mathbb{Q}]$ y se tiene $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Es raro que tengamos $\mathbb{Z}[\alpha] = \mathcal{O}_K$ para algún $\alpha \in \mathcal{O}_K$. Veamos que este es el caso cuando $K = \mathbb{Q}(\zeta_n)$ para $n \in \mathbb{N}$.

Proposición 3.2.25. *Sean p un número primo y $m \in \mathbb{N}$. Entonces $\mathbb{Z}[\zeta_{p^m}]$ es el anillo de enteros de $\mathbb{Q}(\zeta_{p^m})$, es decir, $\mathcal{O}_{\mathbb{Q}(\zeta_{p^m})} = \mathbb{Z}[\zeta_{p^m}]$.*

Demostración. Puesto que $\zeta_{p^m} \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}$ se tiene $\mathbb{Z}[\zeta_{p^m}] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}$. Ahora bien, dado $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}$, puesto que $\{1, \zeta_{p^m}, \dots, \zeta_{p^m}^{\varphi(p^m)-1}\}$ es base de $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$, se tiene que

$$\alpha = \sum_{i=0}^{\varphi(p^m)-1} a_i \zeta_{p^m}^i \quad \text{para} \quad a_i \in \mathbb{Q}. \quad (3.6)$$

Nuestro objetivo es probar que $a_i \in \mathbb{Z}$ y el resultado se seguirá.

Primero recordemos que

$$\begin{aligned} \psi_{p^m}(x) &= \psi_p(x^{p^m-1}) = \prod_{\substack{i=0 \\ (i,p)=1}}^{p^m-1} (x - \zeta_{p^m}^i) \\ &= (x^{p^m-1})^{p-1} + (x^{p^m-1})^{p-2} + \dots + x^{p^m-1} + 1 \end{aligned}$$

y en particular

$$\psi_{p^m}(1) = p = \prod_{\substack{i=0 \\ (i,p)=1}}^{p^m-1} (1 - \zeta_{p^m}^i).$$

Sean i, j primos relativos a p . Entonces existe $t \in \mathbb{Z}$ tal que $it \equiv j \pmod{p^m}$. En particular se sigue que

$$\begin{aligned} \frac{\zeta_{p^m}^j - 1}{\zeta_{p^m}^i - 1} &= \frac{\zeta_{p^m}^{it} - 1}{\zeta_{p^m}^i - 1} = (\zeta_{p^m}^i)^{t-1} + (\zeta_{p^m}^i)^{t-2} + \cdots + (\zeta_{p^m}^i) + 1 \\ &\in \mathbb{Z}[\zeta_{p^m}] \subseteq \mathcal{O} := \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}. \end{aligned}$$

Análogamente $\frac{\zeta_{p^m}^i - 1}{\zeta_{p^m}^j - 1} \in \mathbb{Z}[\zeta_{p^m}]$. De esto se sigue que existe $u \in \mathcal{O}^*$ tal que

$$1 - \zeta_{p^m}^i = u(1 - \zeta_{p^m}^j)$$

y a nivel de ideales de \mathcal{O} se tiene $\langle 1 - \zeta_{p^m}^i \rangle = \langle 1 - \zeta_{p^m}^j \rangle$ para cualesquiera i, j primos relativos a p . Por lo tanto si definimos $\mathfrak{p} := \langle 1 - \zeta_{p^m} \rangle$ se sigue que

$$\langle \psi_{p^m}(1) \rangle = \langle p \rangle = \prod_{\substack{i=0 \\ (i,p)=1}}^{p^m-1} \langle 1 - \zeta_{p^m}^i \rangle = \mathfrak{p}^{\varphi(p^m)}.$$

Puesto que $\varphi(p^m) = [\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}]$, se sigue que p es totalmente ramificado en $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$ y $\mathfrak{p} = \langle 1 - \zeta_{p^m} \rangle$ es un ideal primo de \mathcal{O} .

Se define $v := v_{\mathfrak{p}}$ la valuación correspondiente a \mathfrak{p} , es decir, si $\alpha \in K^*$, $\alpha = \frac{a}{b}$ con $a, b \in \mathcal{O}$ se tiene que $\langle \alpha \rangle = \mathfrak{p}^n \mathfrak{a}$ con \mathfrak{a} un ideal fraccionario de \mathcal{O} primo relativo a \mathfrak{p} y entonces $v_{\mathfrak{p}}(\alpha) := n$. Se tiene que $v_{\mathfrak{p}}$ cumple las mismas propiedades de v_p (ver Definición 3.2.19).

Se tiene que $v(p) = \varphi(p^m)$, $v(\mathfrak{p}) = 1$ y $v(1 - \zeta_{p^m}^i) = 1$ para toda $\text{mcd}(i, p) = 1$.

Ahora bien, puesto que $\mathbb{Q}(\zeta_{p^m}) = \mathbb{Q}(1 - \zeta_{p^m})$ se tiene que $\{1, 1 - \zeta_{p^m}, (1 - \zeta_{p^m})^2, \dots, (1 - \zeta_{p^m})^{\varphi(p^m)-1}\}$ es una base de $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$. Puesto que $\alpha \in \mathcal{O}$, se tiene que $v_{\mathfrak{p}}(\alpha) \geq 0$. Escribamos

$$\alpha = \sum_{\substack{i=0 \\ (i,p)=1}}^{\varphi(p^m)-1} b_i (1 - \zeta_{p^m})^i \quad (3.7)$$

con $b_i \in \mathbb{Q}$. Ahora bien, puesto que $b_i \in \mathbb{Q}$ se tiene que $v(b_i) \equiv 0 \pmod{\varphi(p^m)}$ pues $v(p) = \varphi(p^m)$. Además $v((1 - \zeta_{p^m})^i) = iv(1 - \zeta_{p^m}) = i$ por tanto si $b_i, b_j \neq 0$ y $i \neq j$, se tiene que $v((1 - \zeta_{p^m})^i) \neq v((1 - \zeta_{p^m})^j)$ de donde se sigue que

$$0 \leq v(\alpha) = \min_{i, i \neq 0} \{v((1 - \zeta_{p^m})^i)\} \leq v(b_i) + i \text{ para toda } i \text{ con } b_i \neq 0.$$

Por tanto $v(b_i) \geq -i \in [[1 - \varphi(p^m), 0]]$ y $v(b_i) \equiv 0 \pmod{\varphi(p^m)}$ lo cual implica que $v(b_i) \geq 0$ para toda $0 \leq i \leq \varphi(p^m) - 1$. Esto nos dice en particular que b_i se puede escribir en la forma $b_i = \frac{c_i}{d_i}$ con $c_i, d_i \in \mathbb{Z}$ primos relativos y $p \nmid d_i$ ya que si $p \mid d_i$ entonces $p \nmid c_i$ y $v(b_i) = -v(d_i) < 0$ lo cual es absurdo.

Desarrollando la ecuación (3.7) y regresando a nuestra expresión original (3.6) se tiene

$$\alpha = \sum_{i=0}^{\varphi(p^m)-1} a_i \zeta_{p^m}^i$$

con $v(a_i) \geq 0$. Nuevamente esto significa que si $a_i = \frac{\gamma_i}{\beta_i}$ con $\gamma_i, \beta_i \in \mathbb{Z}$, con $\text{mcd}(\gamma_i, \beta_i) = 1$, $p \nmid \beta_i$. Nuestro objetivo es probar que si algún número primo q divide a β_i , entonces q necesariamente debe ser p . Esto último, junto con lo que hemos probado de que $p \nmid \beta_i$ implican que $\beta_i = 1$ y que $a_i \in \mathbb{Z}$ como deseamos.

Tenemos que $G = G_{p^m} = \text{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}) \cong U_{p^m} = (\mathbb{Z}/p^m\mathbb{Z})^*$ e identificamos cada $\sigma \in G$ con $c \in U_{p^m}$ donde $\sigma(\zeta_{p^m}) = \zeta_{p^m}^c$. De esta forma tenemos para $\sigma \in G$ y denotando $\zeta := \zeta_{p^m}$

$$\alpha^\sigma = \sum_{i=0}^{\varphi(p^m)-1} a_i \zeta_{p^m}^{ci}. \quad (3.8)$$

Formando el vector columna $(\alpha^\sigma)_{\sigma \in G} = \begin{pmatrix} \alpha \\ \vdots \\ \alpha^\sigma \\ \vdots \end{pmatrix}$ y usando la ecuación

(3.8) obtenemos la igualdad (donde el término general $\sigma \in G$ lo identificamos con $c \in U_{p^m}$):

$$\begin{aligned} \begin{pmatrix} \alpha \\ \vdots \\ \alpha^\sigma \\ \vdots \end{pmatrix} &= \begin{pmatrix} 1 & \zeta & \zeta^2 & \dots & \zeta^{\varphi(p^m)-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \zeta^c & \zeta^{2c} & \dots & (\zeta^c)^{\varphi(p^m)-1} \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} = \begin{pmatrix} a_0 \\ \vdots \\ a_{\varphi(p^m)-1} \end{pmatrix} \\ &= A \begin{pmatrix} a_0 \\ \vdots \\ a_{\varphi(p^m)-1} \end{pmatrix} \quad \text{donde} \quad A = (\zeta^{cj})_{\substack{c \in U_{p^m} \\ 0 \leq j \leq \varphi(p^m)-1}} \end{aligned} \quad (3.9)$$

A es una matriz cuadrada $\varphi(p^m) \times \varphi(p^m)$ con coeficientes en $\mathbb{Z}[\zeta]$. Más generalmente se tiene que si B es la *matriz de Vandermonde*

$$B := \begin{pmatrix} 1 & x_1 & \dots & x_1^{r-1} \\ 1 & x_2 & \dots & x_2^{r-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & x_r & \dots & x_r^{r-1} \end{pmatrix}$$

entonces $\det B = \prod_{i < j} (x_i - x_j)$ (damos una demostración al final de la proposición).

Podemos ordenar $U_{p^m} = \{c_1, \dots, c_{p^m}\}$ y poniendo $x_i = \zeta^{c_i}$, $1 \leq i \leq \varphi(p^m)$ y $r = \varphi(p^m)$ se tendrá que $A = \begin{pmatrix} 1 & x_1 & \dots & x_1^{r-1} \\ 1 & x_2 & \dots & x_2^{r-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & x_r & \dots & x_r^{r-1} \end{pmatrix}$ y si $\text{Adj } A$ denota la matriz

adjunta de A , se tiene $A^{-1} = \frac{1}{\det A} (\text{Adj } A)$. Ahora bien, $\det A = \prod_{i < j} (\zeta^{c_i} - \zeta^{c_j})$ y puesto que $\zeta^{c_i} - \zeta^{c_j} = \zeta^{c_i} (1 - \zeta^{c_j - c_i}) = \zeta^{c_i} u_{ij} (1 - \zeta)^{c_i - c_j}$ donde u_{ij} es una unidad de \mathcal{O} se sigue que $\det A = u(1 - \zeta)^t$ para algunos $u \in \mathcal{O}^*$ y

$t \in \mathbb{Z}$. En particular tenemos de (3.9) que $\begin{pmatrix} a_0 \\ \vdots \\ a_{\varphi(p^m)-1} \end{pmatrix} = A^{-1} \begin{pmatrix} \alpha \\ \vdots \\ \alpha^\sigma \\ \vdots \end{pmatrix}$ lo cual

implica que

$$a_i = \frac{(\text{entero algebraico})}{u(1 - \zeta)^t}. \quad (3.10)$$

Puesto que $p = v(1 - \zeta)^{\varphi(p^m)}$ con $v \in \mathcal{O}^*$, multiplicando por cierta unidad $w \in \mathcal{O}^*$ y $(1 - \zeta)^s$ para algún s , se tiene que $a_i = \frac{(\text{entero algebraico})}{p^u} \in \mathbb{Q}$. Por tanto el único primo q que puede dividir a β_i es p y el resultado se sigue. \square

Ahora damos probamos que $\det \begin{pmatrix} 1 & x_1 & \dots & x_1^{r-1} \\ 1 & x_2 & \dots & x_2^{r-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & x_r & \dots & x_r^{r-1} \end{pmatrix} = \prod_{i < j} (x_i - x_j)$. Con-

sideremos variables arbitrarias X, X_2, \dots, X_r y consideremos el polinomio

$f(X) := \det \begin{pmatrix} 1 & X & \dots & X^{r-1} \\ 1 & X_2 & \dots & X_2^{r-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & X_r & \dots & X_r^{r-1} \end{pmatrix} \in F[X]$ donde F es el campo de las funciones

rationales en las variables X_2, \dots, X_r . Entonces $f(X)$ es de grado $r-1$. Puesto que $f(X_2) = \dots = f(X_{r-1}) = 0$, se sigue que $f(X) = D \prod_{j=2}^r (X - X_j)$ don-

de D es el coeficiente líder de f . Entonces $D = \det \begin{pmatrix} 1 & X_2 & \dots & X_2^{r-2} \\ 1 & X_3 & \dots & X_3^{r-2} \\ \vdots & \vdots & \dots & \vdots \\ 1 & X_r & \dots & X_r^{r-2} \end{pmatrix}$. Por

hipótesis de inducción en r , se sigue que $D = \prod_{2 \leq i < j \leq r} (X_i - X_j)$. Definiendo $x_1 := X_1, x_2 := X_2, \dots, x_r := X_r$ se sigue el resultado.

Notemos que puesto que $\{1, \zeta, \dots, \zeta^{\varphi(p^m)-1}\}$ es una base entera de $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}$ sobre \mathbb{Z} , se sigue que

$$\delta_{\mathbb{Q}(\zeta_{p^m})} = (-1)^{\varphi(p^m)/2} \det A^2. \quad (3.11)$$

Calculando $\det A^2$ se seguirá el discriminante.

Proposición 3.2.26. *Con las notaciones anteriores, se tiene*

$$\det A^2 = \pm p^{p^{m-1}(mp-m-1)}.$$

Demostración. Para $c \in \mathbb{Z}$ se tiene $1 - \zeta^c = -\zeta^c(1 - \zeta^{-c})$ por lo que tenemos

$$\det A = \pm \prod_{\substack{0 < k < j < p^m \\ p \nmid kj}} (\zeta^j - \zeta^k) = u_1 \prod_{\substack{0 < k < j < p^m \\ p \nmid kj}} (1 - \zeta^{k-j})$$

donde $u_1 \in \mathcal{O}^*$ y $\det A^2 = u_2 \prod_{\substack{0 < k, j < p^m \\ p \nmid kj, k \neq j}} (1 - \zeta^{k-j})$ con $u_2 \in \mathcal{O}^*$.

Puesto que $\det A^2 \in \mathbb{Z}$ y $u_3(1 - \zeta)^{\varphi(p^m)} = p$ con $u_3 \in \mathcal{O}^*$, se tiene que $\det A^2 = \pm p^s$ para algún $s \in \mathbb{N} \cup \{0\}$. Para calcular s consideremos nuevamente v la valuación asociada a $\mathfrak{p} = \langle 1 - \zeta \rangle$. Ahora bien $\mathfrak{p}^{\varphi(p^m)} = \langle p \rangle$, es decir $v(p) = \varphi(p^m)$ y para $1 \leq n \leq m$, $1 - \zeta_{p^n} = 1 - \zeta_{p^m}^{p^{m-n}} = u_4(1 - \zeta_{p^m})^{p^{m-n}}$, $u_4 \in \mathcal{O}^*$.

Por lo tanto $v(1 - \zeta_{p^n}) = p^{m-n}$. Agrupando los términos $1 - \zeta_{p^m}^{p^{m-n}}$ en la expresión de $\det A^2$ obtenemos

$$\det A^2 = \omega \prod_{n=1}^m (1 - \zeta_{p^m})^{s_{m-n}}$$

donde $\omega \in \mathcal{O}^*$ y $s_i = |\{(k, j) \mid k \equiv j \pmod{p^i}, k \not\equiv j \pmod{p^{i+1}}, p \nmid kj, 0 < k, j < p^m\}|$. Una vez calculado s_i , se tendrá que

$$\varphi(p^m)s = v(\det A^2) = \sum_{n=1}^m s_{m-n} p^{n-m}.$$

Sea $0 < j < \varphi(p^m)$, $p \nmid j$ fijo y sea

$$c_j^{(n)} = \{k \mid 0 < k < p^m, p \nmid k, k \equiv j \pmod{p^n}\}.$$

Consideremos el epimorfismo natural

$$\begin{aligned} \varphi_n: U_{p^m} &\longrightarrow U_{p^n} \\ x \pmod{p^m} &\longmapsto x \pmod{p^n} \end{aligned}$$

con núc $\varphi_n = D_{p^m, p^n} = \{x \in U_{p^m} \mid x \equiv 1 \pmod{p^n}\}$. Entonces, $c_j^{(n)} = \varphi_n^{-1}(\{j\})$ y por tanto $|c_j^{(n)}| = |\text{núc } \varphi_n| = \frac{\varphi(p^m)}{\varphi(p^n)} = p^{m-n}$. Por otro lado tenemos que

$$s_i = \left| \bigcup_{j \in U_{p^m}} (c_j^{(i)} - c_j^{(i+1)}) \right|, \quad 1 \leq i \leq m-2.$$

Se sigue que

$$s_i = \varphi(p^m) \cdot (p^{m-i} - p^{m-i-1}) = \varphi(p^m) p^{m-i-1} (p-1), \quad 1 \leq i \leq m-2.$$

Para $i = m-1$, $s_{m-1} = |\{(k, j) \mid 0 < k, j < p^m, p \nmid kj, k \not\equiv j \pmod{p}\}| = \varphi(p^m)(p-1)$.

Finalmente, para $i = 0$, consideremos s_0 . Se tiene

$$s_0 = |\{(k, j) \mid k \not\equiv j \pmod{p}\}|.$$

Fijando j , $0 < j < p^m$, $p \nmid j$, tenemos que existen p^{m-1} elementos k con $0 < k < p^m$ tales que $k \equiv j \pmod{p}$. Por lo tanto hay $\varphi(p^m) - p^{m-1}$ elementos k tales que $k \not\equiv j \pmod{p}$. Puesto que existen $\varphi(p^m)$ tales elementos j , se sigue que

$$s_0 = \varphi(p^m)(\varphi(p^m) - p^{m-1}) = \varphi(p^m)(p^{m-1}(p-2)).$$

Por tanto

$$\begin{aligned} \varphi(p^m)s &= v(\det A^2) = \sum_{i=0}^{m-1} s_i p^i = \\ &= \varphi(p^m)[p^{m-1}(p-2) + \sum_{i=1}^{m-1} p^{m-i-1}(p-1)p^i] = \\ &= \varphi(p^m)[(p-2)p^{m-1} + (m-1)(p-1)p^{m-1}] = \\ &= \varphi(p^m)p^{m-1}(mp-m-1) \end{aligned}$$

de donde se sigue el resultado. \square

Corolario 3.2.27. *Para un número primo p y $m \in \mathbb{N}$ se tiene $\delta_{\mathbb{Q}(\zeta_{p^m})} = (-1)^{\varphi(p^m)/2} p^{m-1}(mp-m-1)$.* \square

Puesto que los primos ramificados en K/\mathbb{Q} son los primos que dividen a δ_K , donde K es cualquier campo numérico, se tiene

Corolario 3.2.28.

- (I) Si p es un número primo, $m \in \mathbb{N}$, entonces el único primo ramificado en $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$ es p y es totalmente ramificado.
- (II) Para $n \in \mathbb{N}$, $n \geq 3$, $n \not\equiv 2 \pmod{4}$, un número primo p se ramifica en $\mathbb{Q}(\zeta_n)$ si y solamente si p divide a n .

Demostración.

- (I) Es el Corolario 3.2.27.
 (II) Del Corolario 3.2.11, $\mathbb{Q}(\zeta_n) = \prod_{i=1}^r \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ donde la descomposición en primos de n está dada por $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Finalmente un número primo p se ramifica en $\mathbb{Q}(\zeta_n)/\mathbb{Q} \iff$ se ramifica en algún $\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q} \iff p = p_i$ para algún $1 \leq i \leq r \iff p|n$. \square

Para estudiar el anillo $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ con $n \in \mathbb{N}$ arbitrario, salvo que $n \not\equiv 2 \pmod{4}$, veamos que bajo ciertas condiciones para dos extensiones E/\mathbb{Q} y K/\mathbb{Q} , se tiene que $\mathcal{O}_E \mathcal{O}_K = \mathcal{O}_{EK}$.

Primero recordemos que en una torre de campos numéricos $K \subseteq L \subseteq M$, diferente es multiplicativo, esto es,

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \cdot \text{con}_{L/M} \mathfrak{D}_{L/K}$$

donde $\text{con}_{L/M}$ denota a la conorma de L a M , es decir, si \mathfrak{p} es un ideal primo de \mathcal{O}_L y el ideal extendido $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, entonces $\text{con}_{L/M} \mathfrak{p} := \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ y el mapeo se extiende para cualquier ideal fraccionario $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos de \mathcal{O}_L y $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$. Se define $\text{con}_{L/M} \mathfrak{a} := (\text{con}_{L/M} \mathfrak{p}_1)^{\alpha_1} \cdots (\text{con}_{L/M} \mathfrak{p}_r)^{\alpha_r}$.

Notemos que si \mathfrak{a} es un ideal fraccionario de L , entonces $N_{L/M} \text{con}_{L/M} \mathfrak{a} = \mathfrak{a}^{[M:L]}$.

Por otro lado decimos que dos extensiones F/E y H/E son *linealmente disjuntas* sobre E si una base de F/E es también una base de FH/H . Equivalentemente, para extensiones finitas, si $[F : E] = [FH : H]$.

Teorema 3.2.29. Sean K y E dos campos numéricos. Supongamos que los discriminantes de K y E son primos relativos y que K y E son linealmente disjuntos sobre \mathbb{Q} . Entonces

$$\mathcal{O}_{KE} = \mathcal{O}_K \mathcal{O}_E \quad \text{y} \quad \mathfrak{D}_{KE} = \mathfrak{D}_K^{[E:\mathbb{Q}]} \mathfrak{D}_E^{[K:\mathbb{Q}]}.$$

Demostración. Los diferentes satisfacen

$$\mathfrak{D}_{KE/\mathbb{Q}} = \mathfrak{D}_{KE/L} \cdot \text{con}_{K/KE} \mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{KE/E} \cdot \text{con}_{E/KE} \mathfrak{D}_{E/\mathbb{Q}}. \quad (3.12)$$

Ahora bien, se tiene por hipótesis que $\text{con}_{K/KE} \mathfrak{D}_{K/\mathbb{Q}}$ y $\text{con}_{E/KE} \mathfrak{D}_{E/\mathbb{Q}}$ son primos relativos. Por otro lado tenemos

$$\mathfrak{D}_{KE/K} | \text{con}_{E/KE} \mathfrak{D}_{E/\mathbb{Q}} \quad \text{y} \quad \mathfrak{D}_{KE/E} | \text{con}_{K/KE} \mathfrak{D}_{K/\mathbb{Q}}$$

de donde obtenemos que $\mathfrak{D}_{KE/K}$ y $\mathfrak{D}_{KE/E}$ son primos relativos. De la ecuación (3.12) se sigue que

$$\mathfrak{D}_{KE/E} = \text{con}_{K/KE} \mathfrak{D}_{K/\mathbb{Q}} \quad \text{y} \quad \mathfrak{D}_{KE/K} = \text{con}_{E/KE} \mathfrak{D}_{E/\mathbb{Q}}. \quad (3.13)$$

Para obtener una base de \mathcal{O}_{KE} sobre \mathbb{Z} , usaremos las bases complementarias, es decir, las del diferente inverso. Sea W una base de \mathcal{O}_K/\mathbb{Q} y V

una base de \mathcal{O}_E/\mathbb{Z} . Sea W' la base dual de W con respecto a la traza, esto es, si $W = \{w_1, \dots, w_t\}$ entonces $W' = \{w'_1, \dots, w'_t\} \subseteq K$ satisface que $\text{Tr}_{K/\mathbb{Q}}(w'_i w_j) = \delta_{ij}$ para $1 \leq i, j \leq t$. En otras palabras

$$\mathbb{Z}w'_1 + \dots + \mathbb{Z}w'_t = \{x \in K \mid \text{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\} = \mathfrak{D}_{K/\mathbb{Q}}^{-1}$$

y W' genera a $\mathfrak{D}_{K/\mathbb{Q}}^{-1}$ sobre \mathbb{Z} . Se sigue que W' genera $\mathfrak{D}_{KE/K}^{-1}$ sobre \mathcal{O}_K . Entonces el doble dual, $(W')' = W$ genera \mathcal{O}_{KE} sobre \mathcal{O}_E . Por lo tanto $\mathcal{O}_{KE} = \mathcal{O}_E(W) = \mathcal{O}_E\mathcal{O}_K$.

Finalmente

$$\begin{aligned} \mathfrak{d}_{KE/\mathbb{Q}} &= N_{KE/\mathbb{Q}}(\mathfrak{D}_{KE/\mathbb{Q}}) = N_{KE/\mathbb{Q}}(\text{con}_{K/KE} \mathfrak{D}_{K/\mathbb{Q}} \text{con}_{E/KE} \mathfrak{D}_{E/\mathbb{Q}}) \\ &= N_{KE/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}}) N_{KE/\mathbb{Q}}(\mathfrak{D}_{E/\mathbb{Q}}) \\ &= N_{K/\mathbb{Q}}(N_{KE/K} \mathfrak{D}_{K/\mathbb{Q}}) N_{E/\mathbb{Q}}(N_{KE/E} \mathfrak{D}_{E/\mathbb{Q}}) \\ &= N_{K/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}}^{[KE:K]}) N_{E/\mathbb{Q}}(\mathfrak{D}_{E/\mathbb{Q}}^{[KE:E]}) = \mathfrak{d}_{K/\mathbb{Q}}^{[E:\mathbb{Q}]} \mathfrak{d}_{E/\mathbb{Q}}^{[K:\mathbb{Q}]} . \end{aligned} \quad \square$$

El Teorema 3.2.29 nos facilita de manera substancial el cálculo de una base entera de $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ y el discriminante $\delta_{\mathbb{Q}(\zeta_n)}$ donde $n \in \mathbb{N}$, $n > 1$, $n \not\equiv 2 \pmod{4}$.

Teorema 3.2.30. *Se tiene que para $n \in \mathbb{N}$, $\mathbb{Z}[\zeta_n]$ es el anillo de enteros de $\mathbb{Q}(\zeta_n)$, es decir, $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$ es una base entera de $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$.*

Demostración. Esto es consecuencia del Teorema 3.2.29: Se tiene que si p, q son dos primos distintos, $\alpha, \beta \in \mathbb{N}$, entonces $\mathbb{Q}(\zeta_{p^\alpha})$ y $\mathbb{Q}(\zeta_{q^\beta})$ son linealmente disjuntos y que los discriminantes son primos relativos (Corolarios 3.2.11 y 3.2.27). Por lo tanto si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, se tiene que $\mathbb{Q}(\zeta_n) = \prod_{i=1}^r \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ y por lo tanto

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \prod_{i=1}^r \mathcal{O}_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})} = \prod_{i=1}^r \mathbb{Z}[\zeta_{p_i^{\alpha_i}}] = \mathbb{Z}[\zeta_n]. \quad \square$$

Teorema 3.2.31. *Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ es la descomposición en primos de n , entonces el diferente de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ está dado por*

$$\mathfrak{D}_{\mathbb{Q}(\zeta_n)/\mathbb{Z}} = \prod_{i=1}^r \text{con}_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}(\zeta_n)} \mathfrak{p}_i^{p_i^{\alpha_i-1}(p_i\alpha_i-\alpha_i-1)}$$

donde \mathfrak{p}_i es ideal primo de $\mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ dado por $\mathfrak{p}_i = \langle 1 - \zeta_{p_i^{\alpha_i}} \rangle$.

Demostración. Puesto que $\mathfrak{d}_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})} = \langle p_i \rangle^{p_i^{\alpha_i}(p_i\alpha_i-\alpha_i-1)}$ (Corolario 3.2.27) y p_i es totalmente ramificado en $\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}$: $\mathfrak{p}_i^{\varphi(p_i^{\alpha_i})} = \langle p_i \rangle$, entonces el grado relativo $f(\mathfrak{p}_i|p_i)$ es 1 de donde obtenemos que $N_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}} \mathfrak{p}_i = \langle p_i \rangle$.

En particular los diferentes $\mathfrak{D}_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}}$ son primos relativos a pares y $\mathfrak{D}_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}} = \mathfrak{p}_i^{p_i^{\alpha_i-1}(p_i\alpha_i-\alpha_i-1)}$. La conclusión se sigue de la multiplicatividad de los diferentes. \square

Corolario 3.2.32. *Se tiene para $n \in \mathbb{N}$, $n > 1$, $n \not\equiv 2 \pmod{4}$ que*

$$\delta_{\mathbb{Q}(\zeta_n)} = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Demostración. Una primera demostración es usando el Teorema 3.2.31 y el hecho de que $\mathfrak{d}_{\mathbb{Q}(\zeta_n)} = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \mathfrak{d}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$.

Una segunda demostración es usando el Teorema 3.2.29. En ese caso, la igualdad $\mathfrak{d}_{KE} = \mathfrak{d}_K^{[E:\mathbb{Q}]} \mathfrak{d}_E^{[K:\mathbb{Q}]}$ implica $|\delta_{KE}| = |\delta_K|^{[E:\mathbb{Q}]} |\delta_E|^{[K:\mathbb{Q}]}$, la cual a su vez se puede poner en forma aditiva tomando logaritmos:

$$\log |\delta_{KE}| = [E:\mathbb{Q}] \log |\delta_K| + [K:\mathbb{Q}] \log |\delta_E|.$$

Dividiendo entre $[KE:\mathbb{Q}]$, obtenemos

$$\frac{\log |\delta_{KE}|}{[KE:\mathbb{Q}]} = \frac{\log |\delta_K|}{[K:\mathbb{Q}]} + \frac{\log |\delta_E|}{[E:\mathbb{Q}]}.$$
 (3.14)

La ventaja de la expresión (3.14) es que es fácilmente generalizable a una composición de un número finito de campos. En nuestro caso tenemos $\mathbb{Q}(\zeta_n) = \prod_{i=1}^r \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ de donde

$$\begin{aligned} \frac{\log |\delta_{\mathbb{Q}(\zeta_n)}|}{\varphi(n)} &= \frac{\log |\delta_{\mathbb{Q}(\zeta_n)}|}{[\mathbb{Q}(\zeta_n):\mathbb{Q}]} = \sum_{i=1}^r \frac{\log |\delta_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})}|}{[\mathbb{Q}(\zeta_{p_i^{\alpha_i}}):\mathbb{Q}]} = \sum_{i=1}^r \frac{\log |\delta_{\mathbb{Q}(\zeta_{p_i^{\alpha_i}})}|}{\varphi(p_i^{\alpha_i})} \\ &= \sum_{i=1}^r \frac{p_i^{\alpha_i-1} (p_i \alpha_i - \alpha_i - 1) \log p_i}{p_i^{\alpha_i-1} (p_i - 1)} = \sum_{i=1}^r \left(\alpha_i - \frac{1}{\alpha_i - 1} \right) \log p_i \\ &= \sum_{i=1}^r \alpha_i \log p_i - \sum_{i=1}^r \frac{\log p_i}{p_i - 1} = \log n - \sum_{p|n} \frac{\log p}{p-1}. \end{aligned}$$

Por tanto

$$\begin{aligned} \log |\delta_{\mathbb{Q}(\zeta_n)}| &= \varphi(n) \log n - \sum_{p|n} \frac{\varphi(n)}{p-1} \log p = \log n^{\varphi(n)} - \sum_{p|n} \log p^{\varphi(n)/(p-1)} \\ &= \log \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}} \end{aligned}$$

de donde, usando el Teorema 3.2.23 se sigue que

$$\delta_{\mathbb{Q}(\zeta_n)} = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}. \quad \square$$

Uno de los problemas centrales que se estudian en cualquier campo numérico, es su grupo de unidades. En el caso en que $n = p^\alpha$ es una potencia de un

primo, obtuvimos que $\langle p \rangle = \langle 1 - \zeta_{p^\alpha} \rangle^{\varphi(p^\alpha)}$ (ver la demostración de la Proposición 3.2.25). En particular $1 - \zeta_{p^\alpha}$ no puede ser unidad en $\mathbb{Z}[\zeta_{p^\alpha}]$. Resulta ser que cuando n no es potencia de un primo la historia es diferente.

Recordemos que $x^n - 1 = \prod_{d|n} \psi_d(x)$. Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $r \geq 2$ un número natural que no es potencia de un número primo. Entonces

$$f_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + x + 1 = \prod_{\substack{d|n \\ d \neq 1}} \psi_d(x) = \prod_{j=1}^{n-1} (x - \zeta_n^j).$$

Sea $\mathcal{A} := \{d \in \mathbb{N} \mid d|n, d \text{ no es potencia de primo}\}$. Se tiene que $n \in \mathcal{A}$ y $\mathcal{A} \neq \emptyset$. Por otro lado tenemos

$$n = f_n(1) = \prod_{j=1}^{n-1} (1 - \zeta_n^j) = \prod_{i=1}^r \left(\prod_{\beta_i=1}^{\alpha_i} \psi_{p_i^{\beta_i}}(1) \right) \cdot \prod_{d \in \mathcal{A}} \psi_d(1).$$

Ahora bien $\psi_{p_i^{\beta_i}}(1) = p$ para $1 \leq \beta_i \leq \alpha_i$. Por lo tanto

$$\prod_{i=1}^r \prod_{\beta_i=1}^{\alpha_i} \psi_{p_i^{\beta_i}}(1) = \prod_{i=1}^r p_i^{\alpha_i} = n,$$

de donde se sigue que

$$1 = \prod_{d \in \mathcal{A}} \psi_d(1) = \prod_{d \in \mathcal{A}} \prod_{(j,d)=1} (1 - \zeta_d^j).$$

Puesto que $d = n \in \mathcal{A}$, $1 - \zeta_n$ aparece en el producto $\prod_{d \in \mathcal{A}} \psi_d(1)$ y por lo tanto $1 - \zeta_n$ es unidad. En consecuencia, tenemos que $\pm 1 = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1 - \zeta_n) = \prod_{(j,n)=1} (1 - \zeta_n^j)$.

Notemos el siguiente hecho general.

Teorema 3.2.33. *Sea K/\mathbb{Q} una extensión finita de Galois tal que la restricción a K de la conjugación compleja no es trivial, es decir, $J|_K \neq \text{Id}_K$, donde J denota la conjugación compleja. Entonces $N_{K/\mathbb{Q}} K^* \subseteq \mathbb{Q}^+ := \{x \in \mathbb{Q} \mid x > 0\}$.*

Demostración. Sea $G := \text{Gal}(K/\mathbb{Q})$ y sea $H := \{1, J|_K\}$, $|H| = 2$ y $H < G$. Sea $X \subseteq G$ un conjunto de representantes de las clases izquierdas de G módulo H . Entonces $HX = G$ y $G = X \uplus JX$.

Sea $\xi \in K^*$. Se tiene $N_{K/\mathbb{Q}}(\xi) = \prod_{\sigma \in G} \sigma \xi = \left(\prod_{\sigma \in X} \sigma \xi \right) \prod_{\sigma \in X} J(\sigma \xi) = \alpha \bar{\alpha} = |\alpha|^2 > 0$. \square

Resumiendo el desarrollo anterior, tenemos

Teorema 3.2.34. *Si n no es potencia de un número primo, entonces $1 - \zeta_n$ es unidad en $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ y $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1 - \zeta_n) = \prod_{(j,n)=1} (1 - \zeta_n^j) = 1$. \square*

Teorema de Kronecker–Weber

En este capítulo presentamos la demostración del Teorema de Kronecker–Weber usando los grupos de ramificación.

4.1. El teorema y su demostración

El Teorema de Kronecker–Weber establece que toda extensión abeliana de \mathbb{Q} está contenida en algún campo ciclotómico $\mathbb{Q}(\zeta_n)$. El teorema fue originalmente afirmado por Kronecker en 1853 [39]. Sin embargo la prueba estaba incompleta. El mismo Kronecker reconoció que había problemas con el primo $p = 2$. En 1886, Weber casi completó la demostración [76]. Todavía la prueba tenía una laguna, la cual no fue notada sino hasta 95 años después por Olaf Neuman [52]. Finalmente en 1896, D. Hilbert dio una nueva demostración completa de este resultado la cual se basó en los grupos de ramificación [26]. Esta es la primera prueba completa correcta del resultado, aunque el mismo Hilbert no lo supo pues consideró que la prueba de Weber estaba completa.

En la actualidad hay muchas demostraciones, varias de ellas elementales, del Teorema de Kronecker–Weber: reducción al caso local, usando Teoría de Campos de Clase en la cual se usa que un primo p se descompone totalmente en $\mathbb{Q}(\zeta_n) \iff p \equiv 1 \pmod{n}$ lo cual prueba que $\mathbb{Q}(\zeta_n)$ es el campo de clase de rayos correspondiente al “modulus” $(n)\infty$ y toda extensión abeliana de \mathbb{Q} tiene que estar contenida en alguno de estos campos, etc.

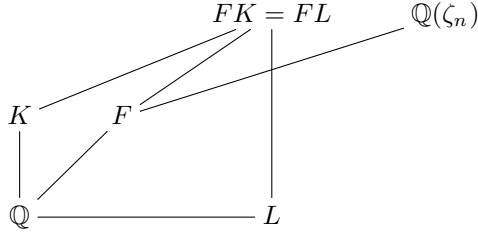
Aquí presentamos una prueba basada en los grupos de ramificación.

Antes que nada recordemos que el Teorema de Minkowski establece que si $1 < [K : \mathbb{Q}] < \infty$, entonces existe un número primo p el cual es ramificado en K/\mathbb{Q} . Como veremos a continuación, el caso central es que si K/\mathbb{Q} es una extensión cíclica de grado p con $p > 2$ un número primo y únicamente se ramifica p , entonces $K \subseteq \mathbb{Q}(\zeta_{p^2})$, esto es, K es la única subextensión de $\mathbb{Q}(\zeta_{p^2})$ de grado p sobre \mathbb{Q} . Similarmente necesitamos el análogo para el caso $p = 2$.

Como primer paso, estudiamos el caso moderadamente ramificado.

Proposición 4.1.1. *Sea K/\mathbb{Q} una extensión abeliana tal que $p \in \mathbb{N}$ es moderadamente ramificado en K . Entonces existe una extensión L de \mathbb{Q} y un subcampo $F \subseteq \mathbb{Q}(\zeta_n)$ para alguna n tal que:*

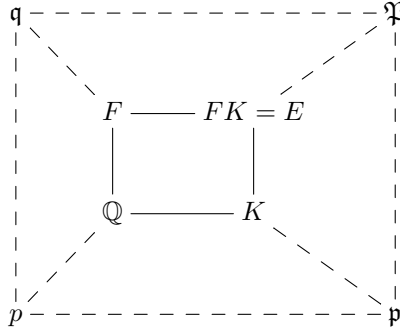
- (a) *Todo primo no ramificado en K es no ramificado en L .*
- (b) *p no se ramifica en L .*
- (c) *$FK = FL$.*



Demostración. Sea \mathfrak{p} un primo en K sobre p . Puesto que p es moderadamente ramificado, el primer grupo de ramificación G_1 de p es trivial. Puesto que K/\mathbb{Q} es abeliana se sigue que el grupo de inercia $I(\mathfrak{p}|p)$ está contenido de manera natural en $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$, Proposición 1.3.12, es decir, el índice de ramificación e de \mathfrak{p}/p divide a $p-1$. En particular $p \neq 2$.

Sea $\zeta := \zeta_p$ y sea F el único subcampo de $\mathbb{Q}(\zeta_p)$ de grado e sobre \mathbb{Q} : $[F : \mathbb{Q}] = e$. Ahora p es moderadamente ramificado en F/\mathbb{Q} puesto que $p \nmid e$ y totalmente ramificado en F/\mathbb{Q} puesto que p es totalmente ramificado en $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

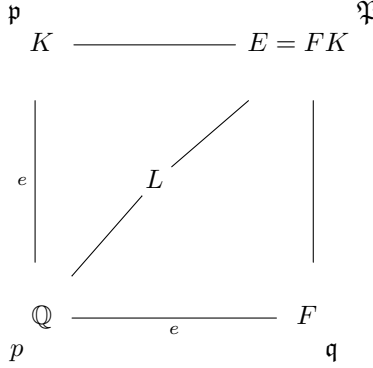
Sea \mathfrak{q} el único primo de F sobre p . Consideremos $FK = E$. Sea \mathfrak{P} un primo en E sobre \mathfrak{p} y sea $I := I(\mathfrak{P}|\mathfrak{p})$ el grupo de inercia. Se tiene $\mathfrak{P} \cap \mathbb{Z} = (p)$ y $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{q}$. Sea $L := E^I$ el subcampo de E fijo bajo I .



Veamos que se cumplen las tres propiedades requeridas en la proposición. Primero, sea $q \in \mathbb{Z}$ un primo no ramificado en K/\mathbb{Q} . Entonces $q \neq p$ y puesto que q no es ramificado en F/\mathbb{Q} , se sigue que q no es ramificado en $E = FK/\mathbb{Q}$. Por tanto q no se ramifica en $L \subseteq E$. Esto es la primera propiedad de L .

Ahora, como L es el campo de inercia de p en E/\mathbb{Q} , p no es ramificado en L/\mathbb{Q} lo cual prueba la segunda propiedad de L .

Queda por demostrar que $FK = FL = E$. Por supuesto $FL \subseteq E$. Se tiene que p es no ramificado en L/\mathbb{Q} y totalmente ramificado en E/L .



Ahora bien, por el Lema de Abhyankar (ver por ejemplo [70, Theorem 12.4.4]) se tiene que

$$e(\mathfrak{P}|p) = [e(\mathfrak{P}|\mathfrak{p}), e(\mathfrak{P}|\mathfrak{q})] = [e, e] = e,$$

esto es, $[E : L] = e$. Por otro lado, como p es totalmente ramificado en F/\mathbb{Q} y no ramificado en L/\mathbb{Q} , se tiene que F y L son linealmente disjuntos sobre \mathbb{Q} y en particular $[FL : L] = [F : \mathbb{Q}] = e$. Por tanto $[E : L] = [FL : L]$. Se sigue que $FL = E = FK$. \square

Corolario 4.1.2. *Sea K/\mathbb{Q} una extensión abeliana tal que todo primo ramificado en K/\mathbb{Q} es moderadamente ramificado. Entonces existe $m \in \mathbb{N}$ tal que $K \subseteq \mathbb{Q}(\zeta_m)$. Más aún, si p_1, \dots, p_r son los primos ramificados en K , se puede seleccionar $m = p_1 \cdots p_r$.*

Demostración. Sean p_1, \dots, p_r todos los primos ramificados en K/\mathbb{Q} . Por la Proposición 4.1.1, existe $F_1 \subseteq \mathbb{Q}(\zeta_{p_1})$ y L_1 tales que p_2, \dots, p_r son los primos ramificados en L_1/\mathbb{Q} y $F_1 K = F_1 L_1$.

Aplicando lo mismo para L_1 , existen $F_2 \subseteq \mathbb{Q}(\zeta_{p_2})$ y L_2 tales que p_3, \dots, p_r son los primos ramificados en L_2 y $F_2 L_1 = F_2 L_2$. Continuando este proceso para $i = 2, \dots, r-1$ se tiene que existen $F_i \subseteq \mathbb{Q}(\zeta_{p_i})$ y L_i tales que p_{i+1}, \dots, p_r son los primos ramificados en L_i y $F_i L_{i-1} = F_i L_i$.

Finalmente, existe $F_r \subseteq \mathbb{Q}(\zeta_{p_r})$ y L_r tales que L_r/\mathbb{Q} es no ramificada y $F_r L_{r-1} = F_r L_r$. Por el Teorema de Minkowski, se tiene que $L_r = \mathbb{Q}$ y por lo tanto $F_r L_{r-1} = F_r$, lo cual implica que $L_{r-1} \subseteq F_r$. Del hecho $F_{r-1} L_{r-2} = F_{r-1} L_{r-1} \subseteq F_r F_{r-1}$ se sigue que $L_{r-2} \subseteq F_r F_{r-1}$. Continuando este proceso, se sigue que

$$K \subseteq F_r F_{r-1} \cdots F_2 F_1 \subseteq \mathbb{Q}(\zeta_{p_1 \cdots p_r}). \quad \square$$

4.2. Caso central: ramificación salvaje

Nuestro siguiente objetivo es probar un resultado análogo al Corolario 4.1.2 en el caso de ramificación salvaje. Primero hagamos un caso particular. Separemos en dos casos: p par y p impar.

Proposición 4.2.1. *Las únicas extensiones cuadráticas de \mathbb{Q} con discriminante una potencia de 2 son $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\sqrt{2}i)$ todas ellas contenidas en $\mathbb{Q}(\zeta_8)$.*

Demostración. Sea $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados. Puesto que $\delta_K = d, 4d$ y por hipótesis $\delta_K = \pm 2^\alpha$, se sigue que necesariamente que $d = \pm 1, \pm 2$. El caso $d = 1$ queda descartado y por lo tanto K es uno de los tipos mencionados en la proposición. El recíproco es igual.

Ahora bien $\zeta_8 = \sqrt{\sqrt{-1}} = \sqrt[4]{-1} = \frac{\cos \pi/4 + \text{sen } \pi/4}{2} = \frac{\sqrt{2}}{2}(1+i)$. Por lo tanto $\zeta_8 + \bar{\zeta}_8 = \sqrt{2}$, $\zeta_8 - \bar{\zeta}_8 = i\sqrt{2}$ de donde se sigue que $\mathbb{Q}(\zeta_4), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_8)$. \square

Proposición 4.2.2. *Sea K/\mathbb{Q} una extensión cíclica de grado p sobre \mathbb{Q} , con p un número primo impar, tal que el único primo ramificado es p . Entonces el diferente de la extensión es igual a $\mathfrak{D}_K = \mathfrak{p}^{2(p-1)}$ donde \mathfrak{p} es el único ideal primo de K sobre p .*

Demostración. Puesto que $[K : \mathbb{Q}] = p$ y p es ramificado, necesariamente tenemos que $e(\mathfrak{p}|p) = p$. Sea $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Se tiene que $v_{\mathfrak{p}}(\pi) = 1$ por lo que $\pi \notin \mathbb{Q}$ puesto que para cualquier $\alpha \in \mathbb{Q}$ tenemos que $v_{\mathfrak{p}}(\alpha) = e(\mathfrak{p}|p)v_p(\alpha) = pv_p(\alpha) \neq 1$.

Se sigue que $K = \mathbb{Q}(\pi)$. Sea

$$f(x) := \text{Irr}(\pi, x, \mathbb{Q}) = x^p + a_{p-1}x^{p-1} + \cdots + a_1x + a_0.$$

Entonces $f(x) \in \mathbb{Z}[x]$ puesto que $\pi \in \mathfrak{p} \subseteq \mathcal{O}_K$, es decir, π es entero. Como $\pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi + a_0 = 0$ con $a_0 \neq 0$, se tiene para $0 \leq i \leq p-1$ que

$$v_{\mathfrak{p}}(a_i\pi^i) = pv_{\mathfrak{p}}(a_i) + i.$$

Si para algún i tuviésemos que $p \nmid a_i$, entonces se tendría que $v_{\mathfrak{p}}(a_i) = 0$ y $v_{\mathfrak{p}}(a_i\pi^i) = i$ y entonces

$$\infty = v_{\mathfrak{p}}(0) = v_{\mathfrak{p}}(\pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi + a_0) = \min_{a_i \neq 0} \{i\} \neq \infty$$

lo cual es absurdo.

Por el Corolario 1.1.3 se tiene que

$$\mathfrak{D}_K = \langle f'(\pi) \rangle = \mathfrak{p}^k \quad \text{donde} \quad k = \sum_{i=0}^{\infty} (|G_i| - 1)$$

donde G_i es el i -ésimo grupo de ramificación correspondiente a \mathfrak{p} sobre p . Puesto que $G_i \subseteq G := \text{Gal}(K|\mathbb{Q})$ y $|G| = p$, se tiene que $|G_i| = p$ ó 1 y por lo tanto $|G_i| - 1 = p - 1$ ó 0 de donde se sigue que $p - 1 | k$.

Ahora, se tiene que $f'(\pi) = p\pi^{p-1} + (p-1)a_{p-1}\pi^{p-2} + \cdots + a_2\pi + a_1$ por lo que para $1 \leq i \leq p$, se tiene para $a_i \neq 0$, donde ponemos $a_p := 1$, que

$$v_{\mathfrak{p}}(ia_i\pi^{i-1}) = v_{\mathfrak{p}}(i) + v_{\mathfrak{p}}(a_i) + i - 1 \equiv (i - 1) \pmod{p}.$$

Por lo tanto si para $i \neq j$ tenemos que $a_i \neq 0$ y $a_j \neq 0$ entonces $v_{\mathfrak{p}}(ia_i\pi^{i-1}) \neq v_{\mathfrak{p}}(ja_j\pi^{j-1})$. Se sigue que

$$k = v_{\mathfrak{p}}(\mathfrak{D}_K) = v_{\mathfrak{p}}(f'(\pi)) = \min_{\substack{1 \leq i \leq p \\ a_i \neq 0}} \{v_{\mathfrak{p}}(ia_i\pi^{i-1})\} = v_{\mathfrak{p}}(i_0) + v_{\mathfrak{p}}(a_{i_0}) + i_0 - 1.$$

Si $i_0 = p$ se tendría $v_{\mathfrak{p}}(pa_p\pi^{p-1}) = v_{\mathfrak{p}}(p\pi^{p-1}) = 2p - 1 \not\equiv 0 \pmod{p-1}$. Por tanto necesariamente $1 \leq i_0 \leq p-1$ y $v_{\mathfrak{p}}(a_{i_0}\pi^{i_0-1}) = pv_p(a_{i_0}) + i_0 - 1 < 2p - 1 = v_{\mathfrak{p}}(pa_p\pi^{p-1})$. Por otro lado $p | a_{i_0}$ lo cual implica que $v_p(a_{i_0}) = t \geq 1$ de donde obtenemos que

$$2p - 1 > v_{\mathfrak{p}}(a_{i_0}\pi^{i_0-1}) = tp + i_0 - 1$$

lo cual implica que $tp < 2p - 1 + 1 - i_0 = 2p - i_0$. Se sigue que $t = 1$ y que $k = p + i_0 - 1 < 2p - 1$.

Por ser ramificación salvaje, se tiene que $k > p - 1$ por lo que $p - 1 < p + i_0 - 1$. Si acaso tuviésemos que $i_0 < p - 1$, entonces $p + i_0 - 1 < 2(p - 1)$ y por ende $p - 1 < k < 2(p - 1)$ lo cual contradice que $p - 1 | k$. Se sigue que $i_0 = p - 1$ y que $k = 2(p - 1)$. \square

El siguiente resultado nos prueba que únicamente existe una extensión cíclica de \mathbb{Q} de grado p ramificado únicamente en p en donde p es un primo impar.

Proposición 4.2.3. *Sea p un número primo con $p > 2$ y sea K/\mathbb{Q} una extensión cíclica de grado p cuyo único primo ramificado es p . Entonces $K \subseteq \mathbb{Q}(\zeta_{p^2})$. Esto es, K es el único subcampo de $\mathbb{Q}(\zeta_{p^2})$ de grado p sobre \mathbb{Q} .*

Demostración. Primero consideremos un campo L tal que L/\mathbb{Q} es una extensión de Galois abeliana y tal que $[L : \mathbb{Q}] = p^2$ donde p es el único primo ramificado. Sea G_0 el grupo de inercia respectivo y sea $L^{G_0} = E$. Entonces p no se ramifica en E/\mathbb{Q} y por tanto E/\mathbb{Q} no es ramificada. Se sigue del Teorema de Minkowski que $E = \mathbb{Q}$ y que $G_0 = G := \text{Gal}(L/\mathbb{Q})$. Ahora bien, si G_1 es el primer grupo de ramificación, entonces por ser la extensión L/\mathbb{Q} salvajemente ramificada se tiene que $G_1 \neq \{e\}$. Consideremos $F := L^{G_1}$. Entonces p es moderadamente ramificado en la extensión F/\mathbb{Q} . Sin embargo, en el caso de que $F \neq \mathbb{Q}$ se tendría que $p | [F : \mathbb{Q}]$ y p necesariamente sería

salvajemente ramificado, lo cual es absurdo. Se sigue que $G_1 = G_0 = G$ y $|G_1| = |G_0| = |G| = p^2$.

Sea G_r el primer grupo de ramificación tal que $|G_r| < p^2$. Puesto que G_{r-1}/G_r es un grupo p -elemental abeliano y puesto que $G_0 = G_1 = G$, se sigue que $r - 1 \geq 1$, esto es, $r \geq 2$. Entonces $G_{r-1}/G_r = G/G_r \subseteq \mathfrak{p}^{r-1}/\mathfrak{p}^r \cong \mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ ya que al ser p totalmente ramificado su grado de inercia es 1.

Se sigue que $|G_{r-1}/G_r| = |G_{r-1}|/|G_r| = p^2/|G_r| \leq p$ y por lo tanto $|G_r| = p$.

Consideremos H cualquier subgrupo de G de orden p y sea $E := L^H$. Sea $\mathfrak{P} := \mathfrak{p} \cap \mathcal{O}_{L^H}$. Entonces por la Proposición 4.2.2 se tiene que $\mathfrak{D}_{L^H/\mathbb{Q}} = \mathfrak{P}^{2(p-1)}$. Por lo tanto

$$\mathfrak{D}_{L/\mathbb{Q}} = \mathfrak{D}_{L^H/L} \text{con}_{L^H/L} \mathfrak{P}^{2(p-1)} = \mathfrak{D}_{L/L^H} \mathfrak{p}^{2p(p-1)}.$$

$$\begin{array}{ccc} & L & \text{---} \text{---} \mathfrak{p} \\ & | & \vdots \\ \mathbb{Q} & \text{---} L^H & \vdots \\ \vdots & & \vdots \\ p & \text{---} \text{---} \text{---} \text{---} \text{---} \mathfrak{P} & \end{array}$$

Se sigue que el diferente $\mathfrak{D}_{L/L^H} = \mathfrak{D}_{L/\mathbb{Q}} \mathfrak{p}^{-2p(p-1)}$ es independiente de H . Ahora bien, si $H \neq G_r$, los grupos de ramificación de L/L^H son

$$G_i \cap H = \begin{cases} H & \text{si } 0 \leq i \leq r-1 \\ 1 & \text{si } i > r \end{cases}$$

de donde

$$\mathfrak{D}_{L/L^H} = \mathfrak{p}^s, \quad s = \sum_{i=0}^{\infty} (|G_i \cap H| - 1) = r(p-1).$$

Por otro lado, si $H = G_r$, se tiene que

$$\mathfrak{D}_{L/L^{G_r}} = \mathfrak{p}^t \quad \text{con} \quad t = \sum_{i=0}^{\infty} (|G_i \cap G_r| - 1) \geq (r+1)(p-1).$$

Estos dos hechos, la independencia de \mathfrak{D}_{L/L^H} de H y que este es máximo exactamente en $H = G_r$ prueban que G tiene un único subgrupo de orden p . Por lo tanto G es cíclico.

Ahora sean K y K' dos extensiones cíclicas de grado p de \mathbb{Q} tales que p es el único primo ramificado. En caso de que $K \neq K'$ se tendría que KK' es una extensión de grado p^2 de \mathbb{Q} donde p es el único primo ramificado. Por lo anterior se seguiría que KK' es una extensión cíclica de \mathbb{Q} pero

$$\text{Gal}(KK'/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(K'/\mathbb{Q}) \cong C_p \times C_p.$$

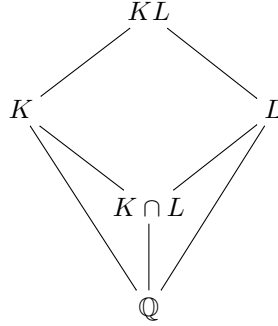
Por tanto, necesariamente $K = K'$ de donde se sigue que hay una única extensión K/\mathbb{Q} cíclica de grado p en donde únicamente p es ramificado.

Finalmente puesto que $\text{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \cong U_{p^2} \cong C_{p-1} \times C_p$, si consideramos $F := (\mathbb{Q}(\zeta_{p^2})^H$ donde H es el subgrupo de U_{p^2} de orden $p-1$, se sigue que $\text{Gal}(F/\mathbb{Q}) \cong C_p$ y p es el único primo ramificado, es decir, $F \subseteq \mathbb{Q}(\zeta_{p^2})$ es el único campo satisfaciendo estas condiciones. \square

Teorema 4.2.4. *Sea p un primo impar. Sea K/\mathbb{Q} una extensión abeliana de grado p^m donde p es único primo ramificado. Entonces $K \subseteq \mathbb{Q}(\zeta_{p^{m+1}})$ y de hecho K es el campo fijo $\mathbb{Q}(\zeta_{p^{m+1}})^H$ donde H es el subgrupo de $U_{p^{m+1}}$ de orden $p-1$: $U_{p^{m+1}} \cong C_{p-1} \times C_{p^m}$. En particular K/\mathbb{Q} es una extensión cíclica.*

Demostración. Sea $L = \mathbb{Q}(\zeta_{p^{m+1}})^H$. Entonces KL es una extensión abeliana de \mathbb{Q} donde p es el único primo ramificado. Se tiene que

$$\begin{aligned} \text{Gal}(KL/\mathbb{Q}) &\subseteq \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \cong C_{p^m} \times C_{p^m} \quad \text{con} \\ \varphi: \text{Gal}(KL/\mathbb{Q}) &\longrightarrow \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \\ \theta &\longmapsto (\theta|_K, \theta|_L). \end{aligned}$$



Si KL/\mathbb{Q} no fuese una extensión cíclica, entonces KL contendría una subextensión de orden p^2 de tipo $C_p \times C_p$ sobre \mathbb{Q} lo cual contradiría la Proposición 4.2.3. Por lo tanto KL/\mathbb{Q} es cíclica. Puesto que $\text{Gal}(KL/\mathbb{Q}) \subseteq C_{p^m}^2$, se sigue que $\text{Gal}(KL/\mathbb{Q}) \cong C_{p^m}$. Por lo tanto $K = L = KL$. \square

Para el primo par $p = 2$ tenemos resultados similares. Primero consideremos una extensión $[K : \mathbb{Q}] = 2$ y 2 es el único primo ramificado. Entonces $K = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ o $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$.

Teorema 4.2.5. *Si K/\mathbb{Q} es una extensión cíclica de grado 2^m , $m \geq 2$, entonces $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$. Más aún K es uno de dos: $K = \mathbb{Q}(\zeta_{2^{m+2}}) \cap \mathbb{R} = \mathbb{Q}(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1}) =: K_m$ o $K = \mathbb{Q}(\zeta_4(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1})) = \mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$.*

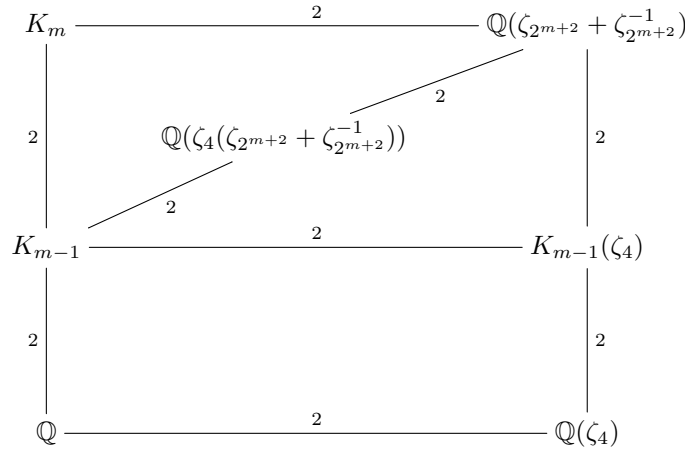
Demostración. Supongamos que K es real, no necesariamente cíclica, únicamente satisfaciendo que K/\mathbb{Q} sea abeliana, que $[K : \mathbb{Q}] = 2^m$ y que 2 es el único primo finito ramificado. Entonces KK_m es una extensión real de \mathbb{Q} donde 2 es el único primo finito ramificado. Nuevamente tenemos que

$$\text{Gal}(KK_m/\mathbb{Q}) \subseteq \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(K_m/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q}) \times C_{2^m}.$$

Si KK_m/\mathbb{Q} no fuese cíclica entonces KK_m tendría una subextensión de tipo $C_2 \times C_2$ sobre \mathbb{Q} pero esta sería real lo cual implicaría que \mathbb{Q} tendría tres extensiones cuadráticas reales donde 2 es el único primo ramificado. Esto contradice que la única extensión cuadrática real de \mathbb{Q} es $\mathbb{Q}(\sqrt{2})$. Se sigue que $K = K_m$ y en particular K es una extensión cíclica de \mathbb{Q} .

Ahora consideremos K no real y sea $M := K(i)$. Sea $M^+ := M \cap \mathbb{R}$. Entonces si $K \neq M$, $K^+ = K_{m-1} \neq M^+$ de donde se sigue que $M^+ = K_m$. Puesto que $M = M^+(i)$, $M = \mathbb{Q}(\zeta_{2^{m+2}})$ y $\text{Gal}(M/\mathbb{Q}) \cong C_2 \times C_{2^m}$. Hay tres subcampos de índice 2, a saber, $\mathbb{Q}(\zeta_{2^{m+1}})$, K_m y $\mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$. Puesto que K/\mathbb{Q} es cíclica y no real, se tiene que $K \neq \mathbb{Q}(\zeta_{2^{m+1}})$ y $K \neq K_m$ por lo que necesariamente $K = \mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$. \square

Observación 4.2.6. El subcampo $\mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$ descrito en el Teorema 4.2.5 es la extensión $\mathbb{Q}(\zeta_4(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1}))$:



Ahora

$$\begin{aligned} \zeta_4(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1}) &= \zeta_4\zeta_{2^{m+2}} + \zeta_4\zeta_{2^{m+2}}^{-1} = \zeta_{2^{m+2}}^{2^m+1} + \zeta_{2^{m+2}}^{2^m-1} \\ &= \zeta_{2^{m+2}}^{2^m+1} + \zeta_{2^{m+2}}^{2^{m+1}-2^m-1} = \zeta_{2^{m+2}}^a + \zeta_{2^{m+2}}^{-a} = \zeta_{2^{m+2}}^a - \zeta_{2^{m+2}}^{-a} \end{aligned}$$

con $\text{mcd}(a, 2) = 1$, por lo que $\mathbb{Q}(\zeta_{2^{m+2}}^a - \zeta_{2^{m+2}}^{-a}) = \mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$.

Con lo anterior ya tenemos todos los elementos para probar:

Teorema 4.2.7 (Kronecker–Weber). *Sea K/\mathbb{Q} una extensión abeliana. Entonces existe $n \in \mathbb{N}$ tal que $K \subseteq \mathbb{Q}(\zeta_n)$.*

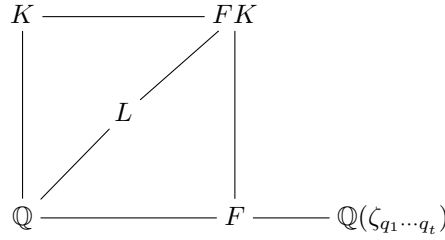
Demostración. Puesto que K/\mathbb{Q} es una extensión abeliana, se tiene que $\text{Gal}(K/\mathbb{Q}) \cong \oplus_{i=1}^r C_{n_i}$ donde cada n_i es potencia de un número primo. Sea $K_i := K^{H_i}$ el campo fijo bajo $H_i := \oplus_{\substack{j=1 \\ j \neq i}}^r C_{n_j}$. Entonces $K = K_1 \cdots K_r$. Si probamos que cada $K \subseteq \mathbb{Q}(\zeta_{m_i})$ entonces

$$K = K_1 \cdots K_r \subseteq \mathbb{Q}(\zeta_{m_1}) \cdots \mathbb{Q}(\zeta_{m_r}) \subseteq \mathbb{Q}(\zeta_{m_1 \cdots m_r}).$$

Por tanto podemos suponer que K/\mathbb{Q} es cíclica de grado p^m con p un número primo.

Por la Proposición 4.1.1, existe una extensión L de \mathbb{Q} y $F \subseteq \mathbb{Q}(\zeta_n)$ para alguna n tal que $FK = FL$ tal que el único primo ramificado en L/\mathbb{Q} es p . De hecho n puede ser tomado como $q_1 \cdots q_t$ donde los primos ramificados de K/\mathbb{Q} son q_1, \dots, q_t y posiblemente p .

Entonces $L \cap F = \mathbb{Q}$ y $\text{Gal}(LF/\mathbb{Q}) \cong \text{Gal}(L/\mathbb{Q}) \times \text{Gal}(F/\mathbb{Q}) \cong \text{Gal}(FK/\mathbb{Q})$.



Entonces por los Teoremas 4.2.4 y 4.2.5 se tiene que $L \subseteq \mathbb{Q}(\zeta_{p^\ell})$ para algún ℓ . Por tanto $K \subseteq FK = FL \subseteq \mathbb{Q}(\zeta_{q_1 \cdots q_t})\mathbb{Q}(\zeta_{p^\ell}) = \mathbb{Q}(\zeta_{p^\ell q_1 \cdots q_t})$. \square

Propiedades y aplicaciones de los campos ciclotómicos

5.1. Caso especial del Teorema de Dirichlet

Una de las aplicaciones interesantes de los campos ciclotómicos es la demostración de un caso particular del Teorema de Dirichlet de números primos en progresiones aritméticas. El Teorema de Dirichlet establece que si $a, b \in \mathbb{Z}$ son primos relativos, entonces existen una infinidad de números primos en la progresión aritmética $a, a + 2b, \dots, a + mb, \dots$. En otras palabras, la congruencia $p \equiv a \pmod{b}$ tiene una infinidad de soluciones para p un número primo.

En la actualidad el Teorema de Dirichlet es una aplicación del Teorema de Densidad de Čebotarev aplicado a los campos ciclotómicos. La demostración original de Dirichlet se basa en la no anulación de una serie L al ser evaluada en $s = 1$. Esto lo veremos más adelante.

El caso particular de $a = 1$, $b = n$ arbitrario ha sido objeto de estudio y existen muchas demostraciones de este caso, incluyendo varias elementales, algunas de ellas de hecho más elementales que la que presentamos aquí. Otro caso especial es $a = -1$, $b = n$. Existe una demostración elemental de este caso debido a E. Landau [41]. Desconocemos si los polinomios ciclotómicos son aplicables a este caso o algún otro, diferente al que desarrollamos a continuación.

Proposición 5.1.1. *Sean p un número primo y $n \in \mathbb{N}$ tal que $p \nmid n$. Sea $a \in \mathbb{Z}$. Entonces*

$$p \mid \psi_n(a) \iff o(a \pmod{p}) = n,$$

es decir, $a^n \equiv 1 \pmod{p}$ y $a^k \not\equiv 1 \pmod{p}$ para $1 \leq k \leq n-1$.

Demostración.

\implies) Primero supongamos que $p \mid \psi_n(a)$. Puesto que $x^n - 1 = \prod_{d \mid n} \psi_d(x)$, se sigue que $a^n - 1 = \prod_{d \mid n} \psi_d(a) \equiv 0 \pmod{p}$ y por lo tanto $a^n \equiv 1 \pmod{p}$. Sea $k := o(a \pmod{p})$. Entonces $k \mid n$. Ahora bien, si $k < n$ tendríamos que $0 \equiv a^k - 1 = \prod_{d \mid k} \psi_d(a) \pmod{p}$. En particular existe $d_0 \mid k$ (y por tanto $d_0 < n$)

tal que $\psi_{d_0}(a) \equiv 0 \pmod{p}$. De esto se sigue que el polinomio $x^n - 1 \pmod{p}$ tiene una raíz múltiple pues $\psi_{d_0}(a) \equiv \psi_n(a) \equiv 0 \pmod{p}$ y $d_0 \neq n$. Sin embargo esto no es posible pues el polinomio $p(x) = (x^n - 1) \pmod{p} \in \mathbb{F}_p[x]$ no tiene raíces múltiples debido a que $p'(x) = nx^{n-1}$ tiene una única raíz, a saber $\alpha = 0 \pmod{p}$ (pues $p \nmid n$) y $0 \pmod{p}$ no es raíz de $p(x)$. Esta contradicción prueba que $o(a \pmod{p}) = n$.

\Leftarrow) Recíprocamente, si $o(a \pmod{p}) = n$, entonces $a^n \equiv 1 \pmod{p}$ pero $a^k \not\equiv 1 \pmod{p}$ para $1 \leq k \leq n-1$. De esto se sigue que

$$a^n - 1 = \prod_{d|n} \psi_d(a) \equiv 0 \pmod{p} \quad \text{y}$$

$$a^k - 1 = \prod_{d|k} \psi_d(a) \not\equiv 0 \pmod{p} \quad \text{para toda } k < n.$$

Por lo tanto $\psi_n(a) \equiv 0 \pmod{p}$. □

Usamos la Proposición 5.1.1 para probar:

Proposición 5.1.2. *Si $p \nmid n$ donde p es un número primo y $n \in \mathbb{N}$, entonces $p|\psi_n(a)$ para algún $a \in \mathbb{Z}$ $\iff p \equiv 1 \pmod{n}$.*

Demostración.

\implies) Si $p|\psi_n(a)$ para algún $a \in \mathbb{Z}$, entonces $o(a \pmod{p}) = n$. Notemos que necesariamente $p \nmid a$. Por lo tanto $n|o(U_p) = p-1$ y por lo tanto $p \equiv 1 \pmod{n}$.
 \Leftarrow) Recíprocamente, como U_p es un grupo cíclico de orden $p-1$, si $p \equiv 1 \pmod{n}$, entonces $n|p-1$ y existe un elemento $\bar{a} \in U_p$ de orden n , es decir $o(a \pmod{p}) = n$, $a \in \mathbb{Z}$. Por la Proposición 5.1.1 se sigue que $p|\psi_n(a)$. □

El caso especial del Teorema de Dirichlet se sigue de este resultado.

Corolario 5.1.3 (Caso especial del Teorema de Dirichlet). *Sea $n \in \mathbb{N}$. Entonces existe una infinidad de números primos p tales que $p \equiv 1 \pmod{n}$.*

Demostración. Supongamos que para un n cualquiera hemos probado la existencia de un primo $p \equiv 1 \pmod{n}$. En este caso $n|p-1$ y por lo tanto $n \leq p-1$. Sea $\alpha \in \mathbb{N}$ tal que $p < n^\alpha$. Por lo probado, existe un número primo q tal que $q \equiv 1 \pmod{n^\alpha}$ y en particular tenemos $q \equiv 1 \pmod{n}$. Entonces $n^\alpha \leq q-1$ y por lo tanto $p < q$. De esta forma se sigue que existe una infinidad de números primos tales que $p \equiv 1 \pmod{n}$. Es decir, basta hallar uno solo de ellos.

Se tiene que para $m \in \mathbb{N}$, $nm \equiv 0 \pmod{n}$ y $\psi_n(nm) \equiv \psi_n(0) \pmod{n}$. Puesto que $\psi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$, se sigue que $\psi_n(0) = \pm 1$. Entonces $\psi_n(nm) \equiv \pm 1 \pmod{n}$. En particular si q es primo tal que $q|n$ entonces $q \nmid \psi_n(nm)$.

Ahora bien, puesto que $\psi_n(x)$ es un polinomio de grado $\varphi(n) \geq 1$ y con coeficiente líder 1, en particular positivo, entonces $\lim_{m \rightarrow \infty} \psi_n(nm) = \infty$.

Sea $m \in \mathbb{N}$ tal que $\psi_n(nm) > 1$ y sea p es un número primo tal que $p|\psi_n(nm)$. Entonces $p \nmid n$ y por la Proposición 5.1.2, se tiene que $p \equiv 1 \pmod{n}$ y esto termina la demostración. □

Observación 5.1.4. La demostración del Corolario 5.1.3 puede hacerse suponiendo que p_1, \dots, p_r son todos los números primos congruentes con 1 módulo n y considerar $mnp_1 \cdots p_r$ y como hicimos, hallamos un primo $p_{r+1} \mid \psi_n(mnp_1 \cdots p_r)$ para alguna $m \geq 1$. Este p_{r+1} es diferente a p_1, \dots, p_r y congruente a 1 mód n . Esta es la demostración de Euclides con $n = 2$. Es decir, se puede considerar el polinomio $\psi_2(x) = x + 1$ para probar que hay una infinidad de primos impares.

Por ejemplo si usamos $\psi_4(x) = x^2 + 1$, probaremos que existen una infinidad de primos de la forma $4n + 1$. Como ejercicio dejamos al lector probar que existen una infinidad de números primos de la forma $8n + 1$ usando el polinomio ciclotómico $\psi_8(x) = x^4 + 1$.

Observación 5.1.5. La Proposición 5.1.2 nos proporciona una manera cómoda de producir primos congruentes con 1 módulo n , pues simplemente evaluamos $\psi_n(a)$ con $a \in \mathbb{Z}$ y todos los factores primos de $\psi_n(a)$ son de esta forma.

Por ejemplo, $\psi_7(4) = \frac{4^7-1}{4-1} = \frac{2^{14}-1}{3} = \frac{16(1024)-1}{3} = \frac{16383}{3} = 5461 = 43 \cdot 127$ y 43 y 127 son ambos primos congruentes con 1 módulo 7.

5.2. Descomposición de primos en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

Para analizar la descomposición de un número primo p en $\mathbb{Q}(\zeta_n)$, $p \nmid n$, veremos cual es el símbolo de Artin asociado a p . Para ello empezamos con

Proposición 5.2.1. Sea p un número primo en \mathbb{Z} y sea \mathfrak{p} un ideal primo en $\mathbb{Q}(\zeta_n)$ que divide a p . Entonces las n -raíces de la unidad son todas distintas módulo \mathfrak{p} .

Demostración. Puesto que $1 + x + \cdots + x^{n-1} = \frac{x^n-1}{x-1} = \prod_{j=1}^{n-1} (x - \zeta_n^j)$ se tiene que evaluando en $x = 1$ obtenemos $n = \prod_{j=1}^{n-1} (1 - \zeta_n^j)$.

Como $p \nmid n$ se sigue que $n \notin \mathfrak{p}$ y por lo tanto $1 - \zeta_n^j \notin \mathfrak{p}$, $j = 1, \dots, n-1$.

Si $\zeta_n^i \equiv \zeta_n^j \pmod{\mathfrak{p}}$ entonces $\zeta_n^i(1 - \zeta_n^{j-i}) \in \mathfrak{p}$. Puesto que ζ_n^i es una raíz de unidad y en particular una unidad, se sigue que $1 - \zeta_n^{j-i} \in \mathfrak{p}$ lo cual implica que $j - i = 0$, es decir, $i = j$. Por tanto, para $1 \leq i, j \leq n-1$, $i \neq j$, entonces $\zeta_n^i \not\equiv \zeta_n^j \pmod{\mathfrak{p}}$. \square

En la situación de la Proposición 5.2.1 se tiene el diagrama

$$\begin{array}{ccccc} \mathfrak{p} & \text{---} & \mathbb{Z}[\zeta_n] & \text{---} & \mathbb{Q}(\zeta_n) \\ & & \downarrow & & \downarrow \\ p & \text{---} & \mathbb{Z} & \text{---} & \mathbb{Q} \end{array}$$

Como $p \nmid n$, entonces \mathfrak{p} no es ramificado en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Sean $\mathcal{O}_{\mathbb{Q}(\zeta_n)}/\mathfrak{p} = \mathbb{Z}[\zeta_n]/\mathfrak{p}$ y $\mathcal{O}_{\mathbb{Q}}/\langle p \rangle = \mathbb{F}_p$ los campos residuales y sea $f := [\mathbb{Z}[\zeta_n]/\mathfrak{p} : \mathbb{F}_p]$.

Entonces $\mathbb{Z}[\zeta_n]/\mathfrak{p} \cong \mathbb{F}_{p^f}$ el campo finito de p^f elementos. El automorfismo de Frobenius $\sigma_p \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ correspondiente a p es (ver Sección 1.3) $\sigma_p = \left[\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}} \right]$ el cual satisface

$$\sigma_p y \equiv y^p \pmod{\mathfrak{p}}, \quad y \in \mathbb{Z}[\zeta_n].$$

En particular, $\sigma_p \zeta_n = \zeta_n^p \pmod{\mathfrak{p}}$.

Por otro lado, para $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, se tiene $\sigma \zeta_n = \zeta_n^a$ con $\text{mcd}(a, n) = 1$ y por la Proposición 5.2.1, $\zeta_n^a \equiv \zeta_n^p \pmod{\mathfrak{p}} \iff a = p$. Se sigue que σ_p está dado por $\sigma_p \zeta_n = \zeta_n^p$.

Así, $\overline{\sigma_p} = \sigma_p \pmod{\mathfrak{p}}$ es generador del grupo cíclico $\text{Gal}(\mathbb{Z}[\zeta_n]/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$ el cual es de orden f . Por tanto

$$\sigma_p^k \zeta_n = \zeta_n^{p^k} = \zeta_n \iff \sigma_p^k = \text{Id} \iff f|k.$$

Es decir f es el mínimo tal que $\zeta_n^{p^f} = \zeta_n$, lo cual equivale a $p^f \equiv 1 \pmod{n}$. Por lo tanto $f = o(p \pmod{n})$.

Puesto que p no es ramificado en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ y $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, si $p\mathbb{Z}[\zeta_n] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, $gf = \varphi(n)$ con $f = o(p \pmod{n})$. Es decir, hemos probado el llamado *Teorema de Reciprocidad Ciclotómica*.

Teorema 5.2.2 (Reciprocidad ciclotómica). *Sea p un primo racional, $n \in \mathbb{N}$. Si $p \nmid n$, entonces si \mathfrak{p} es un primo de $\mathbb{Z}[\zeta_n]$ sobre p se tiene*

$$f = [\mathbb{Z}[\zeta_n]/\mathfrak{p} : \mathbb{F}_p] = o(p \pmod{n})$$

y $g = \varphi(n)/f$ donde $p\mathbb{Z}[\zeta_n] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ primos distintos y $\text{gr } \mathfrak{p}_i = f = o(p \pmod{n})$.

En particular p se descompone totalmente en $\mathbb{Q}(\zeta_n) \iff f = 1 \iff p \equiv 1 \pmod{n}$. \square

Observación 5.2.3. Como mencionamos anteriormente resulta ser que el Teorema de Kronecker–Weber es una consecuencia de la Teoría de Campos de Clases. Ahí se estudian los llamados “módulus” los cuales son productos formales de la forma $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$ donde \mathfrak{p} recorre el conjunto de primos de un campo K el cual, de momento, podemos suponer numérico, $n_{\mathfrak{p}} \in \mathbb{Z}$, $n_{\mathfrak{p}} \geq 0$ para todo \mathfrak{p} y $n_{\mathfrak{p}} = 0$ para casi todo \mathfrak{p} . Si \mathfrak{p} es un primo infinito real, entonces $n_{\mathfrak{p}} = 0$ o 1 y si \mathfrak{p} es un primo infinito imaginario, $n_{\mathfrak{p}} = 0$. Entonces se construye el grupo de clases de ideales de “rayos” correspondientes al modulus \mathfrak{m} el cual se define por $C_{K, \mathfrak{m}} = D_{\mathfrak{m}}/i(K_{\mathfrak{m}, 1})$ donde $D_{\mathfrak{m}}$ son los ideales fraccionarios de \mathcal{O}_K primos relativos a todos los primos finitos que aparecen en \mathfrak{m} , $K_{\mathfrak{m}, 1}$ son los elementos x de $K^* = K \setminus \{0\}$ tales que $x \equiv 1 \pmod{\mathfrak{p}^{n_{\mathfrak{p}}}}$ para cada primo finito que aparece en \mathfrak{m} y tal que $\sigma x > 0$ donde σ representa el encaje correspondiente al primo infinito real \mathfrak{p} que aparece en \mathfrak{m} , es decir, $n_{\mathfrak{p}} = 1$ y finalmente, si $x \in K_{\mathfrak{m}, 1}$, $i(x)$ denota al ideal fraccionario principal generado por x .

Ahora si H es un “*subgrupo de congruencia*”, es decir, si $i(K_{\mathfrak{m},1}) \subseteq H \subseteq D_{\mathfrak{m}}$, entonces el Teorema de Existencia nos dice que existe un campo de clase L/K asociado a H , es decir, existe una única extensión abeliana L de K tal que los primos de \mathcal{O}_K que se descomponen totalmente en L son, salvo un conjunto de densidad 0, los elementos de H . Este es el *campo de clase* asociado a H .

En particular, la máxima extensión abeliana de K es la unión de todos los campos de clase asociados a K .

El Teorema 5.2.2 junto con esta observación nos dice que $\mathbb{Q}(\zeta_m)$ es el campo de clase asociado al modulus $m\infty$ y por tanto la máxima extensión abeliana de \mathbb{Q} es precisamente $\bigcup_{m=1}^{\infty} \mathbb{Q}(\zeta_m)$ de donde obtenemos nuevamente el Teorema de Kronecker-Weber.

Ejemplo 5.2.4. Consideremos $n = 4$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. El único primo finito ramificado en $\mathbb{Q}(\zeta_4)/\mathbb{Q}$ es $p = 2$. Si p es impar, consideremos su clase módulo 4, $p \equiv 1 \pmod{4}$ o $p \equiv 3 \pmod{4} \equiv -1 \pmod{4}$. Entonces si $p \equiv 1 \pmod{4}$, $f = 1$ y por lo tanto $g = \frac{\varphi(4)}{1} = 2$, es decir, $p\mathbb{Z}[i] = \mathfrak{p}\bar{\mathfrak{p}}$. Si $p \equiv -1 \pmod{4}$, $p^2 \equiv 1 \pmod{4}$ y por lo tanto $f = 2$, $g = 1$ y en este caso $p\mathbb{Z}[i] = \mathfrak{p} = \langle p \rangle$ permanece primo.

Ahora $\mathbb{Z}[i]$ es un anillo euclideo con la norma:

$$N(a + bi) = a^2 + b^2 = (a + bi)(a - bi), \quad a, b \in \mathbb{Z}.$$

En particular $\mathbb{Z}[i]$ es de ideales principales. Sea $p \equiv 1 \pmod{4}$, $p\mathbb{Z}[i] = \mathfrak{p}\bar{\mathfrak{p}} = \langle \alpha \rangle \langle \beta \rangle$. Se tiene $N\alpha = N\beta = p$.

Si $\alpha = a + bi$, $p = a^2 + b^2$, es decir p es suma de dos cuadrados; por ejemplo: $13 = 2^2 + 3^2$; $5 = 1^2 + 2^2$; $17 = 1^2 + 4^2$; $29 = 2^2 + 5^2$; etc.

Si $p \equiv 3 \pmod{4}$, la congruencia $a^2 + b^2 \equiv 3 \pmod{4}$ no tiene solución, pues para cualesquiera $a, b \in \mathbb{Z}$, se tiene $a^2 + b^2 \equiv 0, 1, 2 \pmod{4}$ por lo que $p \equiv 3 \pmod{4}$ no es suma de cuadrados.

Finalmente, para $p = 2$, p es ramificado por lo que $2\mathbb{Z}[i] = \mathfrak{p}^2$. Si $\gamma = a + bi$ genera \mathfrak{p} , se tiene $N\gamma = a^2 + b^2 = 2$ lo cual implica que $\gamma = \pm 1 \pm i$. Además $2 = 1^2 + 1^2$.

De lo anterior, dejamos deducir al lector que $m \in \mathbb{N}$ es suma de dos cuadrados: $m = a^2 + b^2$, $a, b \in \mathbb{Z}$ si y solamente si $m = 2^\alpha p_1 \cdots p_r t^2$ donde $\alpha \in \mathbb{N} \cup \{0\}$, $t \in \mathbb{N}$, $r \geq 0$, p_1, \dots, p_r son primos congruentes con 1 módulo 4.

Ejemplo 5.2.5. Sea $n = 23$. Se tiene que U_{23} es un grupo cíclico de orden 22. Empezando por 2, directamente se calcula que $\langle 2 \pmod{23} \rangle = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$ y $o(2 \pmod{23}) = 11$. Entonces puesto que $5^2 \equiv 2 \pmod{23}$, se sigue que 5 módulo 23 genera U_{23} , es decir 5 es raíz 23-ésima primitiva. De lo anterior y puesto que $\varphi(22) = 10$, se sigue que los generadores de U_{23} serán:

$$\{5, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}\} = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}.$$

Así, $x \in U_{23}$ satisface

$$\begin{aligned}
o(x) = 1 &\iff x \equiv 1 \pmod{23}, \\
o(x) = 2 &\iff x \equiv -1 \pmod{23} \equiv 22 \pmod{23}, \\
o(x) = 11 &\iff x \in \{2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \pmod{23}, \\
o(x) = 22 &\iff x \in \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\} \pmod{23}.
\end{aligned}$$

Así p , un número primo en \mathbb{Z} , se descompone totalmente en $\mathbb{Q}(\zeta_{23}) \iff p \equiv 1 \pmod{23}$; p se descompone en 11 factores $\iff p \equiv 22 \pmod{23}$; p se descompone en 2 factores $\iff p \equiv x \pmod{23}$ con $x \in \{2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ y finalmente p permanece primo en $\mathbb{Z}[\zeta_{23}] \iff p \equiv y \pmod{23}$ donde $y \in \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$.

Ahora que conocemos la máxima extensión abeliana de \mathbb{Q} , establecemos cual es su grupo de Galois. Primero recordemos

Teorema 5.2.6. *Sean p un primo impar. Sea $\mathbb{Q}^{(p)} := \bigcup_{n=0}^{\infty} \mathbb{Q}(\zeta_{p^n})$. Entonces*

$$G^{(p)} := \text{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \cong C_{p-1} \times \mathbb{Z}_p$$

donde \mathbb{Z}_p es el anillo de los enteros p -ádicos.

Demostración. Se tiene que $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong U_{p^n} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ y se tiene el diagrama conmutativo

$$\begin{array}{ccc}
\text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) & \xrightarrow{\text{rest}_{n+1}} & \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \\
\downarrow \theta_{n+1} & & \downarrow \theta_n \\
U_{p^{n+1}} & \xrightarrow{\pi_{n+1}} & U_{p^n}
\end{array}$$

donde rest_{n+1} es el mapeo restricción: $\text{rest}_{n+1}(\sigma) = \sigma|_{\mathbb{Q}(\zeta_{p^n})}$ y π_{n+1} es la proyección natural $\pi_{n+1}(x \pmod{p^{n+1}}) = x \pmod{p^n}$. Notemos que $\pi_{n+1}|_{\mathbb{Z}/(p-1)\mathbb{Z}} = \text{Id}_{\mathbb{Z}/(p-1)\mathbb{Z}}$.

Entonces

$$\begin{aligned}
G^{(p)} &:= \text{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q}) = \text{Gal}\left(\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) = \text{Gal}\left(\varinjlim_n \mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \\
&\cong \varprojlim_{n, \text{rest}_{n+1}} \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong \varprojlim_{n, \pi_{n+1}} U_{p^n} \\
&\cong \varprojlim_{n, \pi_{n+1}} (\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}) \\
&\cong (\mathbb{Z}/(p-1)\mathbb{Z}) \times \varprojlim_{\pi_{n+1}} (\mathbb{Z}/p^{n-1}\mathbb{Z}) \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p \cong C_{p-1} \times \mathbb{Z}_p.
\end{aligned}$$

□

El resultado análogo para $p = 2$ es:

Teorema 5.2.7. Sea $\mathbb{Q}^{(2)} := \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})$. Entonces

$$G^{(2)} := \text{Gal}(\mathbb{Q}^{(2)}/\mathbb{Q}) \cong C_2 \times \mathbb{Z}_2.$$

Demostración. Es igual a la demostración del Teorema 5.2.6 considerando que $U_{2^n} \cong C_2 \times C_{2^{n-2}}$ y $\text{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}) \cong U_{2^n}$ donde el primer factor C_2 de U_{2^n} está generado por la conjugación compleja. \square

Los Teoremas 5.2.6 y 5.2.7 nos dan

Teorema 5.2.8. Sea \mathbb{Q}^{ab} la máxima extensión abeliana de \mathbb{Q} . Entonces

$$\begin{aligned} G_{\text{ab}} &:= \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \prod_{\substack{p \text{ primo} \\ p > 2}} (\mathbb{Z}/(p-1)\mathbb{Z}) \times \prod_{p \text{ primo}} \mathbb{Z}_p \\ &\cong C_2 \times \prod_{p \text{ impar}} C_{p-1} \times \hat{\mathbb{Z}}. \end{aligned}$$

Demostración. Por el Teorema de Kronecker-Weber se tiene que $\mathbb{Q}^{\text{ab}} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$. Para cada $n \in \mathbb{N}$, sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su descomposición en primos. Entonces $U_n \xrightarrow{\delta} U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}$ donde

$$\begin{aligned} \delta: U_n &\longrightarrow U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}} \\ x \text{ mód } n &\longmapsto (x \text{ mód } p_1^{\alpha_1}, \dots, x \text{ mód } p_r^{\alpha_r}). \end{aligned}$$

A nivel de grupos de Galois, $\mathbb{Q}(\zeta_n) = \prod_{i=1}^r \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ y $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\varphi} \prod_{i=1}^r \text{Gal}(\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q})$ donde φ está dado por la restricción: $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\varphi(\sigma) = (\sigma|_{\mathbb{Q}(\zeta_{p_1^{\alpha_1}})}, \dots, \sigma|_{\mathbb{Q}(\zeta_{p_r^{\alpha_r}})})$ y se tiene el diagrama conmutativo

$$\begin{array}{ccc} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\varphi} & \prod_{i=1}^r \text{Gal}(\mathbb{Q}(\zeta_{p_i^{\alpha_i}})/\mathbb{Q}) \\ \downarrow \theta_n & & \downarrow (\theta_{p_1^{\alpha_1}}, \dots, \theta_{p_r^{\alpha_r}}) \\ U_n & \xrightarrow{\delta} & \prod_{i=1}^r U_{p_i^{\alpha_i}} \end{array}$$

Por tanto se tiene los isomorfismos

$$\begin{aligned} \varprojlim_n \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\cong \varprojlim_n U_n, \\ \varprojlim_n U_n &\cong \prod_{p \text{ primo}} \left(\varprojlim_{\alpha(p)} U_{p^{\alpha(p)}} \right) \quad \text{y} \\ \varprojlim_n \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\cong \prod_{p \text{ primo}} \left(\varprojlim_{\alpha(p)} \text{Gal}(\mathbb{Q}(\zeta_{p^{\alpha(p)}})/\mathbb{Q}) \right). \end{aligned}$$

Estos tres isomorfismos y los Teoremas 5.2.6 y 5.2.7 nos dan

$$\begin{aligned}
G_{\text{ab}} &= \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) = \text{Gal}\left(\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \\
&\cong \text{Gal}\left(\left(\varinjlim_n \mathbb{Q}(\zeta_n)\right)/\mathbb{Q}\right) \cong \varprojlim_n \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\
&\cong \prod_{p \text{ primo}} \left[\varprojlim_{\alpha(p)} \text{Gal}(\mathbb{Q}(\zeta_{p^{\alpha(p)}})/\mathbb{Q}) \right] \cong \prod_{p \text{ primo}} \left[\varprojlim_{\alpha(p)} U_{p^{\alpha(p)}} \right] \\
&\cong \varprojlim_n U_n \cong \varprojlim_m U_{2^m} \times \prod_{\substack{p \text{ primo} \\ p > 2}} \varprojlim_m U_{p^m} \\
&\cong C_2 \times \mathbb{Z}_2 \times \prod_{p > 2} (C_{p-1} \times \mathbb{Z}_p) \cong C_2 \times \prod_{p > 2} C_{p-1} \times \prod_{p \text{ primo}} \mathbb{Z}_p.
\end{aligned}$$

Finalmente, se tiene $\prod_{p \text{ primo}} \mathbb{Z}_p \cong \hat{\mathbb{Z}}$. □

Ejemplo 5.2.9. Se sabe que únicamente hay 30 campos ciclotómicos con número de clase 1. En este ejemplo estudiaremos $\mathbb{Q}(\zeta_{23})$ el cual es el primer campo ciclotómico con número de clase mayor a 1.

Primero consideremos $\mathbb{Q}(\sqrt{-23})$. Ahora bien, $\mathbb{Q}(\zeta_{23})$ tiene un único subcampo cuadrático K : $K = \mathbb{Q}(\zeta_{23})^H$ donde H es el único subgrupo de U_{23} de orden 11, de hecho $H \cong \langle 2 \text{ mód } 23 \rangle \cong \langle \sigma \in \text{Gal}(\mathbb{Q}(\zeta_{23})/\mathbb{Q}) \mid \sigma\zeta_{23} = \zeta_{23}^2 \rangle$.

Ahora si $\mathbb{Q}(\sqrt{d})$ es este subcampo, entonces 23 es el único primo ramificado en $\mathbb{Q}(\sqrt{d})$ por lo que $\delta_{\mathbb{Q}(\sqrt{d})} = \pm 23 = d$. Puesto que $23 \equiv 3 \text{ mód } 4$ y $-23 \equiv 1 \text{ mód } 4$ se sigue que $d = -23$ y $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-23})$. En otras palabras $\mathbb{Q}(\sqrt{-23}) \subseteq \mathbb{Q}(\zeta_{23})$.

La base entera de $\mathbb{Q}(\sqrt{-23})/\mathbb{Q}$ es $\{1, \frac{1+\sqrt{-23}}{2}\}$. Si ponemos $\alpha := \frac{1+\sqrt{-23}}{2}$, entonces $\text{Irr}(\alpha, x, \mathbb{Q}) = x^2 - x + 6 = f(x)$. Se tiene $f(x) \text{ mód } 2 = x^2 - x = x(x-1)$. Por el Teorema de Kummer se tiene que $2\mathcal{O}_{\mathbb{Q}(\sqrt{-23})} = \mathfrak{p}\bar{\mathfrak{p}}$ donde

$$\mathfrak{p} = \left\langle 2, \frac{1 + \sqrt{-23}}{2} \right\rangle = \langle 2, \alpha \rangle, \quad \bar{\mathfrak{p}} = \left\langle 2, \frac{-1 + \sqrt{-23}}{2} \right\rangle = \langle 2, \bar{\alpha} \rangle = \langle 2, 1 - \alpha \rangle.$$

Por el Ejemplo 5.2.5, se tiene que $2\mathbb{Z}[\zeta_{23}] = \mathfrak{P}\bar{\mathfrak{P}}$. Por lo tanto $\mathfrak{p}\mathbb{Z}[\zeta_{23}] = \mathfrak{P}$ y $\bar{\mathfrak{p}}\mathbb{Z}[\zeta_{23}] = \bar{\mathfrak{P}}$ donde los grados relativos $f(\mathfrak{P}|\mathfrak{p})$ y $f(\bar{\mathfrak{P}}|\bar{\mathfrak{p}})$ son igual a 1. En particular la norma $N := N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}}$ satisface $N\mathfrak{P} = \mathfrak{p}$ y $N\bar{\mathfrak{P}} = \bar{\mathfrak{p}}$.

Se tiene $\langle 2 \rangle \mathbb{Z}[\zeta_{23}] = \langle 2, \alpha \rangle \langle 2, \bar{\alpha} \rangle = \langle 2, \alpha \rangle \langle 2, 1 - \alpha \rangle$. Ahora bien

$$N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}} \mathfrak{P} = \langle 2 \rangle^{11} = N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}} N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})} \mathfrak{P} = N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}} \mathfrak{p}^{11}.$$

Veamos que \mathfrak{p} no es principal. Sea $\beta = a + b\alpha = a + b\left(\frac{1+\sqrt{-23}}{2}\right) \in \mathbb{Z}[\alpha] = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$, $a, b \in \mathbb{Z}$. Entonces $N\beta = (a+b)^2 + 5b^2 - ab$, es decir, $N\beta = 2$ no tiene solución para $a, b \in \mathbb{Z}$.

En caso de que \mathfrak{p} fuese principal, digamos $\mathfrak{p} = \langle \beta \rangle$, entonces $N\mathfrak{p} = \langle 2 \rangle = \langle N\beta \rangle$ y por lo tanto $0 < N\beta = \beta\bar{\beta} = 2$ lo cual es imposible. Por lo tanto \mathfrak{p} no es principal y el número de clase de $\mathbb{Q}(\sqrt{-23})$ es mayor a 1.

Ahora bien, si $\beta = 1 + \frac{1+\sqrt{-23}}{2}$, entonces $N\beta = 8 = 2^3$. Por tanto

$$\mathfrak{p}^3 = \langle \beta \rangle = \left\langle 1 + \frac{1+\sqrt{-23}}{2} \right\rangle = \left\langle \frac{3+\sqrt{-23}}{2} \right\rangle$$

es principal pues $\beta \in \mathfrak{p}^3$, $\langle 2 \rangle = \langle N\beta \rangle \subseteq \langle 2 \rangle$. Se sigue \mathfrak{P} no es principal pues $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}\mathfrak{P} = \mathfrak{p}$ y \mathfrak{P}^3 si lo es pues $\mathfrak{p}^3\mathbb{Z}[\zeta_{23}] = \beta\mathbb{Z}[\zeta_{23}] = \mathfrak{P}^3 = \langle \beta \rangle$. De esto se sigue que 3 divide al número de clase de $\mathbb{Q}(\zeta_{23})$ y $\mathbb{Q}(\zeta_{23})$ no tiene número de clase 1.

Ahora bien, nos falta describir el tipo de descomposición de un primo p en $\mathbb{Q}(\zeta_n)$ cuando $p|n$. Sin embargo esto se sigue de lo que ya sabemos hasta ahora. Como de costumbre suponemos que $n \not\equiv 2 \pmod{4}$.

Sean $p|n$, $a \geq 1$, $a \in \mathbb{N}$ tal que $p^a|n$ y $p^{a+1} \nmid n$, lo cual lo escribiremos $p^a||n$. Entonces por la Proposición 3.2.7 se tiene

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^a})\mathbb{Q}(\zeta_{n/p^a}), \quad \mathbb{Q}(\zeta_{p^a}) \cap \mathbb{Q}(\zeta_{n/p^a}) = \mathbb{Q}.$$

Entonces, puesto que p es totalmente ramificado en $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$ y no ramificado en $\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}$, se tiene que

$$\begin{aligned} e &= \varphi(p^a) = p^{a-1}(p-1), \\ f &= o(p \text{ mód } n/p^a), \\ g &= \frac{\varphi(n/p^a)}{o(p \text{ mód } n/p^a)}. \end{aligned}$$

Resumimos esto en el siguiente resultado.

Teorema 5.2.10. *Sea $n \in \mathbb{N}$, $n > 1$, $n \not\equiv 2 \pmod{4}$. Sea p un primo y sea a la potencia exacta de p que divide a n : $p^a|n$, $p^{a+1} \nmid n$ ($p^a||n$), $a \geq 0$. Entonces si*

$$p\mathbb{Z}[\zeta_n] = \mathfrak{p}_1^e \cdots \mathfrak{p}_g^e, \quad [\mathbb{Z}[\zeta_n]/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = f$$

con $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ primos distintos, se tiene

$$\begin{aligned} e &= \varphi(p^a) = p^{a-1}(p-1), \\ f &= o(p \text{ mód } n/p^a), \\ g &= \frac{\varphi(n/p^a)}{o(p \text{ mód } n/p^a)}. \end{aligned} \quad \square$$

Ahora veamos los grupos de inercia y de descomposición de un primo \mathfrak{P} en $\mathbb{Q}(\zeta_n)$ sobre p . Sea $p^a||n$. Entonces se tiene que si $I := I(\mathfrak{P}|p)$ y $D := D(\mathfrak{P}|p)$ son los grupos de inercia y de descomposición de \mathfrak{P} sobre p en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, entonces

$$|I| = e = \varphi(p^a) = p^{a-1}(p-1),$$

$$|D| = ef = p^{a-1}(p-1) \cdot o(p \bmod n/p^a).$$

Ahora bien, si $\mathfrak{p} := \mathfrak{P} \cap \mathbb{Q}(\zeta_{n/p^a})$, se tiene que $\mathfrak{P}/\mathfrak{p}$ es totalmente ramificado y \mathfrak{p}/p es no ramificado.

$$\begin{array}{ccc}
 \mathfrak{P} & \mathbb{Q}(\zeta_n) & \\
 & \downarrow & \left. \vphantom{\begin{array}{c} \mathbb{Q}(\zeta_n) \\ \downarrow \end{array}} \right\} \mathfrak{P}/\mathfrak{p} \text{ es totalmente ramificado} \\
 \mathfrak{p} & \mathbb{Q}(\zeta_{n/p^a}) & \\
 & \downarrow & \left. \vphantom{\begin{array}{c} \mathbb{Q}(\zeta_{n/p^a}) \\ \downarrow \end{array}} \right\} \mathfrak{p}/p \text{ es no ramificado} \\
 p & \mathbb{Q} &
 \end{array}$$

Por lo tanto $I = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a}))$. Por otro lado, puesto que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^a}) \cdot \mathbb{Q}(\zeta_{n/p^a})$ y $\mathbb{Q}(\zeta_{p^a}) \cap \mathbb{Q}(\zeta_{n/p^a}) = \mathbb{Q}$, se tiene

$$\begin{aligned}
 \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})) \times \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{p^a})) \quad \text{y} \\
 \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})) &\cong \text{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}); \\
 \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{p^a})) &\cong \text{Gal}(\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}).
 \end{aligned}$$

$$\begin{array}{ccccc}
 & & \mathbb{Q}(\zeta_n) & & \\
 & \swarrow & & \searrow & \\
 \mathbb{Q}(\zeta_{p^a}) & & & & \mathbb{Q}(\zeta_{n/p^a}) \\
 & \searrow & & \swarrow & \\
 & & \mathbb{Q} & &
 \end{array}$$

En particular $I \cong \text{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong U_{p^a}$.

Otra descripción de I la podemos obtener mediante la sucesión exacta de grupos abelianos:

$$1 \longrightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})) \longrightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\text{rest}} \text{Gal}(\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}) \longrightarrow 1.$$

Con los isomorfismos $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{h} U_n$ y $\text{Gal}(\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}) \xrightarrow{k} U_{n/p^a}$ y la proyección natural

$$\begin{aligned}
 \pi: U_n &\longrightarrow U_{n/p^a} \\
 x \bmod n &\longmapsto x \bmod n/p^a,
 \end{aligned}$$

y núc $\pi = D_{n,n/p^a} = \{x \bmod n \mid x \equiv 1 \bmod n/p^a\}$ obtenemos el siguiente diagrama conmutativo donde las filas son exactas

$$\begin{array}{ccccccc}
1 & \longrightarrow & \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})) & \xrightarrow{i} & \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\text{rest}} & \text{Gal}(\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}) \longrightarrow 1 \\
& & \downarrow h' & & \downarrow h & & \downarrow k \\
1 & \longrightarrow & D_{n,n/p^a} & \xrightarrow{j} & U_n & \xrightarrow{\pi} & U_{n/p^a} \longrightarrow 1
\end{array}$$

donde i, j son las inyecciones naturales y h' es el mapeo restricción de h a $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a}))$. Entonces

$$I = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})) \cong D_{n,n/p^a} \cong U_{p^a} \cong \text{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}).$$

Por otro lado, el grupo de descomposición de \mathfrak{p}/p en $\mathbb{Q}(\zeta_{n/p^a})/\mathbb{Q}$ está dado por el automorfismo de Frobenius $\sigma_p(\zeta_{n/p^a}) = \zeta_{n/p^a}^p$ el cual corresponde a $p \bmod (n/p^a)$ y es de orden f . El grupo de descomposición $D(\mathfrak{P}|p)$ es isomorfo a $D(\mathfrak{p}|p) \times I(\mathfrak{P}|p)$ y por tanto a $\langle p \bmod (n/p^a) \rangle \times U_{p^a}$.

Precisemos un poco más al grupo $D(\mathfrak{P}|p)$. Se tiene que $D(\mathfrak{P}|p) = \langle \sigma, I(\mathfrak{P}|p) \rangle$ donde $\sigma|_{\mathbb{Q}(\zeta_{n/p^a})}$ satisface $\bar{\sigma}(\zeta_{n/p^a}) = \zeta_{n/p^a}^p$. Digamos que $\sigma(\zeta_n) = \zeta_n^b$ con $\text{mcd}(b, n) = 1$. Entonces se tiene

$$\zeta_n^{bp^a} = \sigma(\zeta_n^{p^a}) = \sigma(\zeta_{n/p^a}) = \zeta_{n/p^a}^b = \zeta_{n/p^a}^p,$$

lo cual implica que $b \equiv p \bmod (n/p^a)$.

Puesto que $\text{mcd}(p^a, n/p^a) = 1$, por el Teorema Chino del Residuo, se tiene que existe $b \in \mathbb{Z}$ tal que $b \equiv p \bmod (n/p^a)$ y $b \equiv \alpha \bmod p^a$ con $\text{mcd}(\alpha, p) = 1$, por ejemplo $\alpha = 1$. Sea $d = \text{mcd}(b, n)$. Veamos que $d = 1$. Si $d \neq 1$, existe un número primo que divide a d . Si $p \mid d$ entonces $p \mid b$ y de la congruencia $b \equiv p \bmod n/p^a$ se sigue que $p \mid n/p^a$ lo cual es absurdo. Por tanto existe un primo $q \neq p$ tal que $q \mid d$. Puesto que $d \mid n$, y $q \neq p$, se sigue que $q \mid (n/p^a)$ y además $q \mid b$. De la congruencia $b \equiv p \bmod (n/p^a)$ se sigue que $q \mid p$ lo cual es absurdo. En resumen $d = \text{mcd}(b, n) = 1$.

Seleccionamos b de la discusión anterior satisfaciendo $b \equiv p \bmod (n/p^a)$ y $b \equiv 1 \bmod p^a$. Entonces tenemos que $o(p \bmod (n/p^a)) = o(b \bmod (n/p^a)) = f$ y puesto que $b^i \equiv 1 \bmod p^a$ para toda i , se sigue que $o(b \bmod n) = f$. Sea σ dado por esta b , es decir, $\sigma(\zeta_n) = \zeta_n^b$. Entonces veamos que $\langle \sigma \rangle \cap D_{n,n/p^a} = \{1\}$ pues si $\sigma^j \in D_{n,n/p^a}$ entonces $b^j \equiv 1 \bmod (n/p^a)$ lo cual implica que $f \mid j$ y por tanto $\sigma^j = \text{Id}$. Hemos obtenido que

$$D(\mathfrak{P}|p) \cong \langle b \rangle \times D_{n,n/p^a} \cong \langle \sigma \rangle \times \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p^a})).$$

Teorema 5.2.11. *Con las notaciones anteriores se tiene que para cualquier $n \in \mathbb{N}$ y para cualquier número primo p en \mathbb{Z} , si p^a es la potencia exacta de p que divide a n , tenemos*

$$\begin{aligned}
I(\mathfrak{P}|p) &\cong I(\mathfrak{p}|p) \cong D_{n,n/p^a} \cong U_{p^a}, \\
D(\mathfrak{P}|p) &\cong D(\mathfrak{p}|p) \times I(\mathfrak{P}|p) \cong \langle p \bmod n/p^a \rangle \times U_{p^a}. \quad \square
\end{aligned}$$

Para explicitar los generadores de los ideales primos de \mathfrak{P} sobre un primo p en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, usamos el Teorema de Kummer 1.1.4.

En el caso $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, en la notación del Teorema de Kummer, tenemos $A = \mathbb{Z}$, $\text{coc } A = \mathbb{Q}$, $E = \mathbb{Q}(\zeta_n)$ y $B = \mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, $\text{Irr}(x, \zeta_n, \mathbb{Q}) = \psi_n(x)$, $\psi_n(x) \bmod p = \overline{\psi_n(x)} = (\overline{P_1(x)} \cdots \overline{P_g(x)})^e$, entonces $p\mathbb{Z}[\zeta_n] = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, $\mathfrak{P}_i = \langle p, P_i(\zeta_n) \rangle$.

En el caso particular de $p \equiv 1 \bmod n$, p se descompone totalmente, $\psi_n(x) = \prod_{(i,n)=1} (x - \zeta_n^i)$, $\overline{\psi_n(x)} = (x - a_1) \cdots (x - a_{\varphi(n)})$, $P_i(x) = x - a_i \in \mathbb{Z}[x]$, $1 \leq i \leq \varphi(n)$ para algunos $a_i \in \mathbb{Z}$ tales que $a_i \bmod p = n$ y $\mathfrak{P}_i = \langle p, \zeta_n - a_i \rangle$, $P_i(\zeta_n) = \zeta_n - a_i$.

5.3. Subcampos de $\mathbb{Q}(\zeta_n)$

Por el Teorema de Kronecker–Weber, toda extensión abeliana finita de \mathbb{Q} está contenida en algún $\mathbb{Q}(\zeta_n)$. Por tanto conocer la aritmética de los subcampos de $\mathbb{Q}(\zeta_n)$ equivale a conocer la aritmética de las extensiones abelianas finitas de \mathbb{Q} .

Primero notemos que si K/\mathbb{Q} es cualquier extensión de Galois y si J es la conjugación compleja, entonces para $j := J|_K$, $j = \text{Id} \iff K \subseteq \mathbb{R}$. En caso de que $j \neq \text{Id}$, $K^j = K \cap \mathbb{R} =: K^+$ y $[K : K^+] = 2$. El campo K^+ se llama el *campo real* de K .

Notemos que lo anterior no se cumple cuando K/\mathbb{Q} no es de Galois. Por ejemplo, si $K := \mathbb{Q}(\zeta_n \sqrt[n]{2})$, con $n \in \mathbb{N}$, $n \geq 3$, entonces $K^+ = K \cap \mathbb{R} = \mathbb{Q}$ y $[K : K^+] = [K : \mathbb{Q}] = n$.

Sea $K := \mathbb{Q}(\zeta_n)$. Entonces $J|_{\mathbb{Q}(\zeta_n)} = j$ se identifica con $-1 \in U_n$. Entonces

Lema 5.3.1. *Se tiene*

$$\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n + \bar{\zeta}_n) = \mathbb{Q}\left(2 \cos \frac{2\pi}{n}\right).$$

$$\text{Además } \text{Irr}(\zeta_n, x, \mathbb{Q}(\zeta_n)^+) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1.$$

Demostración. Sea $\alpha = \zeta_n + \zeta_n^{-1} = \frac{\zeta_n^2 + 1}{\zeta_n}$. Por tanto $\zeta_n^2 - \zeta_n \alpha + 1 = 0$. En particular, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha)(\zeta_n)$, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] \leq 2 = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+]$. El resultado se sigue del hecho de que $\alpha \in \mathbb{R}$. \square

Ahora bien $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+) = \{1, J\} \cong \{\pm 1\}$, donde J es la conjugación compleja la cual es identificada con $-1 \in U_n$. Se tiene $\text{Gal}(\mathbb{Q}(\zeta_n)^+/\mathbb{Q}) \cong U_n/\{\pm 1\}$.

Para cualquier $n \geq 3$, $n \not\equiv 2 \bmod 4$, se tiene que $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ es ramificada en todos los primos infinitos pues todos los primos infinitos de $\mathbb{Q}(\zeta_n)^+$ son reales y todos los primos infinitos en $\mathbb{Q}(\zeta_n)$ son complejos. En el caso de los primos finitos, tenemos una diferencia entre si n es potencia de un número primo y cuando n es dividido por al menos dos números primos distintos.

Teorema 5.3.2.

- (1) Si $n = p^m$ donde p es primo y $m \in \mathbb{N}$, entonces $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ es ramificada en los primos de $\mathbb{Q}(\zeta_n)^+$ encima de p y en los primos infinitos y es no ramificada en ningún otro primo.
- (2) Si n es dividido por al menos dos primos distintos, $n \not\equiv 2 \pmod{4}$, entonces $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ es ramificada únicamente en los primos infinitos, es decir, es no ramificada en todos los primos finitos.

Demostración. Puesto que si $n = p^m$, p es totalmente ramificada en $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$, solo falta probar que ningún primo finito se ramifica en $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ cuando n es dividido por al menos primos distintos.

Sean p, q dos números primos impares distintos que dividen a n o p impar y $q = 4$. Entonces $\zeta_p, \zeta_q \in \mathbb{Q}(\zeta_n) \setminus \mathbb{Q}(\zeta_n)^+$. Por tanto $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_p) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_q) = \mathbb{Q}(\zeta_n)^+(\zeta_p) = \mathbb{Q}(\zeta_n)^+(\zeta_q)$.

Ahora bien, al adjuntar ζ_p a $\mathbb{Q}(\zeta_n)^+$ el único primo finito posible a ramificarse en $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n)^+(\zeta_p)/\mathbb{Q}(\zeta_n)^+$ es p pero p no es ramificado en $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n)^+(\zeta_q)/\mathbb{Q}(\zeta_n)^+$ pues el único primo finito posible a ramificarse en esta última extensión es q si q es impar o 2 si $q = 4$. Por lo tanto $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ es no ramificado en los primos finitos. \square

5.3.1. Subcampos de $\mathbb{Q}(\zeta_{2^m})$

Consideremos los subcampos de $\mathbb{Q}(\zeta_{2^m})$ con $m \geq 2$. En este caso, tenemos que $\text{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}) \cong U_{2^m} \cong C_2 \times C_{2^{m-2}}$. Recordemos que la sucesión exacta

$$1 \longrightarrow D_{2^m,4} \longrightarrow U_{2^m} \xrightarrow{\pi} U_4 \longrightarrow 1$$

donde π es el epimorfismo natural, se escinde pues $D_{2^m,4}$ es cíclico de orden 2^{m-2} que es de orden maximal en U_{2^m} . Además, aunque esto no es necesario, se tiene que $D_{2^m,4}$ es generado por $1 + 2^2 = 5$ y $U_4 = \{\pm 1\}$. El encaje natural $i: U_4 \rightarrow U_{2^m}$, $i(-1) = -1$, satisface $\pi \circ i = \text{Id}_{U_4}$ y por tanto es el mapeo de escisión. En otras palabras, $U_{2^m} \cong U_4 \times D_{2^m,4} \cong C_2 \times C_{2^{m-2}}$.

Sean $\langle a \rangle = U_4 \cong C_2$, $\langle b \rangle = D_{2^m,4} \cong C_{2^{m-2}}$. Notemos que $\mathbb{Q}(\zeta_{2^m})^{U_4} = \mathbb{Q}(\zeta_{2^m})^{\{1,J\}} = \mathbb{Q}(\zeta_{2^m})^+$ y $\mathbb{Q}(\zeta_{2^m})^{D_{2^m,4}} = \mathbb{Q}(\zeta_{2^m})^{\text{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}(\zeta_4))} = \mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_{2^m})^+ & \xrightarrow{U_4 = \langle a \rangle \cong \{1,J\}} & \mathbb{Q}(\zeta_{2^m}) \\ \downarrow & & \downarrow \text{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}(\zeta_4)) \cong D_{2^m,4} \cong C_{2^{m-2}} \cong \langle b \rangle \\ \mathbb{Q} & \xrightarrow{U_4} & \mathbb{Q}(\zeta_4) \end{array}$$

Los subgrupos de orden 2^r de U_{2^m} con $1 \leq r \leq m-1$ son:

- (1) $r = m-1$: $U_{2^m} = \langle a, b \rangle$;

(2) $1 \leq r \leq m-1$:

- $\langle a, b^{2^{m-1-r}} \rangle = U_4 \times D_{2^m, 2^{m+1-r}} \cong C_2 \times C_{2^{r-1}}$;
- $\langle b^{2^{m-2-r}} \rangle = D_{2^m, 2^{m-r}} \cong C_{2^r}$;
- $\langle ab^{2^{m-2-r}} \rangle \cong C_{2^r}$.

Los respectivos campos fijos son:

- (1) $\mathbb{Q}(\zeta_{2^m})^{U_{2^m}} = \mathbb{Q}$;
- (2)
 - $\mathbb{Q}(\zeta_{2^m})^{U_4 \times D_{2^m, 2^{m+1-r}}} \cong \mathbb{Q}(\zeta_{2^{r+2}})^+$;
 - $\mathbb{Q}(\zeta_{2^m})^{D_{2^m, 2^{m-r}}} = \mathbb{Q}(\zeta_{2^{r+1}})^+(\zeta_4) = \mathbb{Q}(\zeta_{2^{r+1}})$;
 - $\mathbb{Q}(\zeta_{2^m})^{\langle ab^{2^{m-2-r}} \rangle} = \mathbb{Q}(\zeta_4(\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1})) = \mathbb{Q}(\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1})$
 (pues $b^{2^{m-r-2}}(\zeta_{2^{r+2}}) = \zeta_{2^{r+2}}$ y $a(\zeta_{2^{r+2}}) = -\zeta_{2^{r+2}}$ por lo que $\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1}$ queda fijo bajo $ab^{2^{m-2-r}}$ y $\mathbb{Q}(\zeta_{2^{r+2}})/\mathbb{Q}(\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1})$ es de grado 2).

Podemos hacer más explícita la descripción de estos subcampos. Sea $\alpha_r = \zeta_{2^r} + \zeta_{2^r}^{-1}$. Entonces $\alpha_r^2 = \zeta_{2^{r-1}} + \zeta_{2^{r-1}}^{-1} + 2 = \alpha_{r-1} + 2$, esto es, $\alpha_r = \sqrt{\alpha_{r-1} + 2}$ donde escogemos el signo positivo pues $\alpha_r > 0$. Entonces tenemos

$$\begin{aligned}\zeta_{2^3} + \zeta_{2^3}^{-1} &= \zeta_8 + \zeta_8^{-1} = \sqrt{2}; \\ \zeta_{2^4} + \zeta_{2^4}^{-1} &= \sqrt{2 + \sqrt{2}};\end{aligned}$$

y en general

$$\zeta_{2^m} + \zeta_{2^m}^{-1} = \underbrace{\sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}}_{m-2} = \alpha_m.$$

Por tanto tenemos:

Teorema 5.3.3. Para $1 \leq r \leq m-2$, $\mathbb{Q}(\zeta_{2^m})$ tiene tres subcampos de grado 2^r sobre \mathbb{Q} :

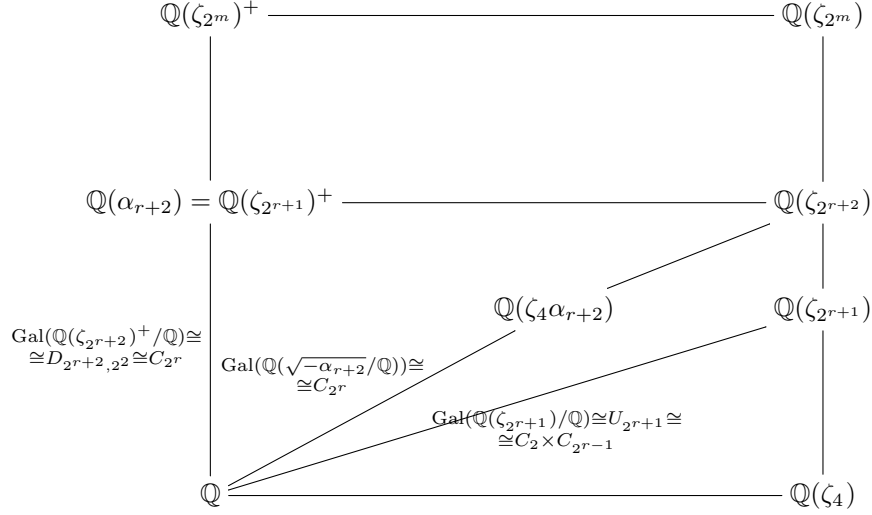
- $\mathbb{Q}(\zeta_{2^{r+2}})^+ = \mathbb{Q}(\alpha_{r+2})$;
- $\mathbb{Q}(\zeta_{2^{r+1}})$;
- $\mathbb{Q}(\zeta_4(\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1})) = \mathbb{Q}(\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1}) = \mathbb{Q}(\sqrt{-\alpha_{r+2}})$

donde $\alpha_{r+2} = \underbrace{\sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}}_r$. Más aún tanto el primer como el

tercer campo son extensiones cíclicas de \mathbb{Q} e inclusive el segundo campo para el caso $r = 1$. En el caso $r \geq 2$,

$$\begin{aligned}\text{Gal}(\mathbb{Q}(\alpha_{r+2})/\mathbb{Q}) &= \text{Gal}(\mathbb{Q}(\zeta_{2^{r+2}})^+/\mathbb{Q}) \cong D_{2^{r+2}, 2^2} \cong C_{2^r}; \\ \text{Gal}(\mathbb{Q}(\sqrt{-\alpha_{r+2}})/\mathbb{Q}) &\cong C_{2^r}; \\ \text{Gal}(\mathbb{Q}(\zeta_{2^{r+1}})/\mathbb{Q}) &\cong \langle 1, J \rangle \times \langle D_{2^{r+1}, 2^2} \rangle \cong \langle \pm 1 \rangle \times \langle D_{2^{r+1}, 2^2} \rangle.\end{aligned}$$

En el caso $r = 1$, las extensiones son cíclicas de grado 2 y estas son $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ y $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$. \square

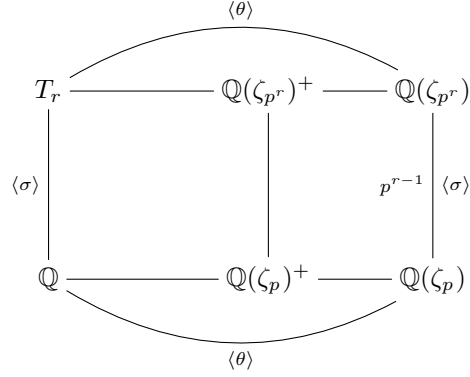


5.3.2. Subcampos de $\mathbb{Q}(\zeta_{p^m})$, p primo, $p > 2$

En el caso en que p es impar, $\text{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \cong U_{p^r}$ es cíclico, $U_{p^r} \cong C_{p-1} \times C_{p^{r-1}}$, de orden $\varphi(p^r) = p^{r-1}(p-1)$.

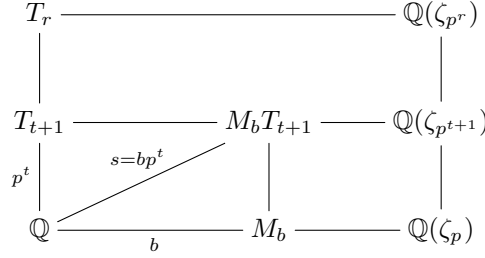
Un elemento de orden p^{r-1} en U_{p^r} es $1+p$ el cual corresponde a $\sigma\zeta_{p^r} = \zeta_{p^r}^{1+p} = \zeta_{p^r}\zeta_{p^{r-1}}$. Consideremos una raíz primitiva módulo p , digamos a , es decir, $U_p = \langle a \rangle$ y sea $\theta(\zeta_p) = \zeta_p^a$. Pongamos $\text{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) = \langle \theta, \sigma \rangle$ donde extendemos a θ como una extensión de $\theta(\zeta_p) = \zeta_p^a$ a $\theta(\zeta_{p^r})$ y $o(\theta) = p-1$. Por ejemplo, si $\theta(\zeta_{p^r}) = \zeta_{p^r}^a$, entonces $\zeta_{p^r}^{p^{r-1}a} = \zeta_p^a = \theta(\zeta_p) = \theta(\zeta_{p^{r-1}}) = \zeta_{p^{r-1}}^{p^{r-1}a}$. Es decir $p^{r-1}a \equiv p^{r-1}\alpha \pmod{p^r}$, $a \equiv \alpha \pmod{p}$. Además $\theta^{p-1}(\zeta_{p^r}) = \zeta_{p^r}^{a^{p-1}} = \zeta_{p^r}$, esto es $a^{p-1} \equiv 1 \pmod{p^r}$. Es decir $\theta(\zeta_{p^r}) = \zeta_{p^r}^a$, $o(a \pmod{p^r}) = p-1$.

Sea $T_r := \mathbb{Q}(\zeta_{p^r})^{\langle \theta \rangle}$, $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{p^r})^{\langle \theta \rangle}$.



$$\begin{aligned} \mathbb{Q}(\zeta_{p^r}) &= T_r \mathbb{Q}(\zeta_p) = T_r(\zeta_p); \quad T_r \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}; \\ \mathbb{Q}(\zeta_{p^r})^+ &= T_r \mathbb{Q}(\zeta_p)^+ = T_r(\zeta_p + \zeta_p^{-1}); \quad T_r \subseteq \mathbb{R}. \end{aligned}$$

Notemos que si $s|p^r$, entonces escribiendo $s = bp^t$ con $t \leq r-1$ y $b|p-1$. Por unicidad de las extensiones de \mathbb{Q} contenidas en $\mathbb{Q}(\zeta_{p^r})$ pues U_{p^r} es cíclico, el único campo de grado s contenido en $\mathbb{Q}(\zeta_{p^r})$ es $M_b T_{t+1}$ donde M_b es el único subcampo de $\mathbb{Q}(\zeta_p)$ de grado b sobre \mathbb{Q} .



A continuación describiremos de manera más o menos explícita los campos M_b y T_{t+1} en general. Empezamos con M_b . Sea $c := \frac{p-1}{b}$. Se tiene $[\mathbb{Q}(\zeta_p) : M_b] = c$, $[M_b : \mathbb{Q}] = b$, $bc = p-1$.

Notemos que M_b es el campo fijo bajo el subgrupo de U_p de orden c , es decir, bajo $\langle \theta^b \rangle$ ya que $o(\theta^b) = c$ y $\text{Gal}(M_b/\mathbb{Q}) \cong \frac{\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_p)/M_b)} = \frac{\langle \theta \rangle}{\langle \theta^b \rangle} = \langle \theta \text{ mód } \theta^b \rangle = \langle \bar{\theta} \rangle$. Esto es, $M_b = \mathbb{Q}(\zeta_p)^{\langle \theta^b \rangle}$.

Puesto que en general se tiene que $\theta \zeta_p = \zeta_p^a$, entonces $\theta^j \zeta_p = \zeta_p^{a^j}$. Consideremos $\mu := \zeta_p + \theta^b \zeta_p + \dots + \theta^{(c-1)b} \zeta_p$. Así $\theta^b \mu = \theta^b \zeta_p + \theta^{2b} \zeta_p + \dots + \theta^{cb} \zeta_p = \mu$, es decir, $\mu \in \mathbb{Q}(\zeta_p)^{\langle \theta^b \rangle} = M_b$ y por lo tanto $[\mathbb{Q}(\mu) : \mathbb{Q}] \leq [M_b : \mathbb{Q}] = b$.

Ahora bien, $\mu = \sum_{i=0}^{c-1} \theta^{ib} \zeta_p = \sum_{i=0}^{c-1} \zeta_p^{a^{ib}}$ y se tiene $\theta \mu = \sum_{i=0}^{c-1} (\theta \zeta_p)^{a^{ib}} = \sum_{i=0}^{c-1} \zeta_p^{a^{ib+1}} = \sum_{i=0}^{c-1} (\zeta_p^{a^{ib}})^a$ y en general $\theta^j \mu = \sum_{i=0}^{c-1} (\zeta_p^{a^{ib}})^{a^j} = \sum_{i=0}^{c-1} \zeta_p^{a^{ib+j}}$. Se sigue que $\theta^j \mu \neq \mu$ para $1 \leq j \leq b-1$. De hecho tenemos que como a es una raíz primitiva módulo p , se tiene que $\{a^{ib+j} \mid 0 \leq i \leq c-1, 0 \leq j \leq b-1, (i,j) \neq (0,0)\} = \{a^1, \dots, a^{p-1}\}$ son todos distintos módulo p y

$\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$ es base de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, por lo que $\mu, \theta\mu, \dots, \theta^{b-1}\mu$ son b conjugados distintos de μ de donde obtenemos $[\mathbb{Q}(\mu) : \mathbb{Q}] \geq b$.

Se sigue que $M_b = \mathbb{Q}(\mu)$, donde $\mu = \sum_{i=0}^{c-1} \zeta_p^{a^{ib}}$. Ahora bien, de esta misma forma tenemos que $T_r = \mathbb{Q}(\delta)$, donde

$$\delta = \zeta_{p^r} + \theta\zeta_{p^r} + \dots + \theta^{p-2}\zeta_{p^r} = \zeta_{p^r} + \zeta_{p^r}^\alpha + \dots + \zeta_{p^r}^{\alpha^{p-2}} = \sum_{i=0}^{p-2} \zeta_{p^r}^{\alpha^i}$$

donde $o(\alpha \bmod p^r) = p-1$ y se tiene $\sigma\delta = \sum_{i=0}^{p-2} (\sigma\zeta_{p^r})^{\alpha^i} = \sum_{i=0}^{p-2} \zeta_{p^r}^{(1+p)\alpha^i}$.

Para T_{t+1} , $t \leq r-1$, se tiene $T_{t+1} = \mathbb{Q}(\delta_{t+1})$ donde $\delta_{t+1} = \sum_{i=0}^{p-2} \zeta_{p^{t+1}}^{\alpha^i}$ con $o(\alpha \bmod p^{t+1}) = p-1$.

Teorema 5.3.4. *Sean $p > 2$ un primo impar y $m \in \mathbb{N}$. Los subcampos de $\mathbb{Q}(\zeta_{p^m})$ están dados por*

$$M_b \cdot T_r, \quad b|p-1, \quad 0 \leq r \leq m-1,$$

donde

$$\begin{aligned} M_b &= \mathbb{Q}(\mu_b), \quad T_r = \mathbb{Q}(\delta_r), \quad \mu_b = \sum_{i=0}^{c-1} \zeta_p^{a^{ib}}, \quad \delta_r = \sum_{i=0}^{p-2} \zeta_{p^r}^{\alpha^i}, \\ o(a \bmod p) &= p-1, \quad o(\alpha \bmod p^r) = p-1, \quad c = \frac{p-1}{b}, \\ [M_b : \mathbb{Q}] &= b, \quad [T_r : \mathbb{Q}] = p^r. \end{aligned}$$

Además

$$\begin{aligned} \text{Gal}(M_b/\mathbb{Q}) &= \langle \bar{\theta} \rangle \cong C_b, \quad \text{Gal}(T_r/\mathbb{Q}) = \langle \bar{\sigma} \rangle \cong C_{p^r}, \\ \theta(\zeta_p) &= \zeta_p^a, \quad \sigma(\zeta_{p^m}) = \zeta_{p^m}^{1+p}, \quad \bar{\theta} = \theta \bmod \langle \theta^b \rangle, \quad \bar{\sigma} = \sigma \bmod \langle \sigma^{p^r} \rangle. \quad \square \end{aligned}$$

En particular se tiene que $\mathbb{Q}(\zeta_{p^m})^+$ es de grado $\frac{\varphi(p^m)}{2} = \frac{p-1}{2}p^{m-1}$, esto es, $\mathbb{Q}(\zeta_{p^m})^+ = M_{(p-1)/2}T_{m-1}$. Notemos que $M_{(p-1)/2} = \mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\mu_{(p-1)/2})$, $\mu_{(p-1)/2} = \zeta_p + \zeta_p^{-1}$. En otras palabras tenemos $\mathbb{Q}(\zeta_{p^m})^+ = \mathbb{Q}(\zeta_p)^+T_{m-1}$.

5.3.3. Subcampos cuadráticos

Sea p un primo impar. Entonces $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ el cual es un número par y $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong U_p \cong C_{p-1}$. Por tanto existe un único subcampo cuadrático $K \subseteq \mathbb{Q}(\zeta_p)$, es decir, $[K : \mathbb{Q}] = 2$. Se tiene que el único primo finito ramificado en $\mathbb{Q}(\zeta_p)$ es p , lo cual implica que el único primo finito ramificado en K/\mathbb{Q} es p . Escribiendo $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados, necesariamente $4 \nmid \delta_K$ pues 2 no es ramificado. Por esto, tenemos $\delta_K = d = \pm p$ y puesto que $4 \nmid \delta_K$, se sigue que $d \equiv 1 \bmod 4$. Entonces

$$d = \begin{cases} p & \text{si } p \equiv 1 \pmod{4} \\ -p & \text{si } p \equiv 3 \pmod{4} \end{cases} = (-1)^{(p-1)/2} p.$$

Así, es subcampo cuadrático de $\mathbb{Q}(\zeta_p)$ es $\mathbb{Q}\left(\sqrt{(1)^{\frac{p-1}{2}} p}\right)$.

Otra forma de probar que $\mathbb{Q}\left(\sqrt{(1)^{\frac{p-1}{2}} p}\right) \subseteq \mathbb{Q}(\zeta_p)$ es la siguiente. Consideremos $\psi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \dots + x + 1 = \prod_{i=1}^{p-1} (1 - \zeta_p^i)$, por lo que $p = \psi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta_p^i)$. Para $\frac{p+1}{2} \leq j \leq p-1$, esto es, $j = p-i$ con $1 \leq i \leq \frac{p-1}{2}$, se tiene

$$1 - \zeta_p^j = 1 - \zeta_p^{p-i} = 1 - \zeta_p^{-i} = 1 - \frac{1}{\zeta_p^i} = \zeta_p^{-i}(\zeta_p^i - 1) = -\zeta_p^{-i}(1 - \zeta_p^i),$$

por lo que

$$\begin{aligned} p &= \prod_{i=1}^{p-1} (1 - \zeta_p^i) = \prod_{i=1}^{(p-1)/2} (1 - \zeta_p^i) \cdot \prod_{i=1}^{(p-1)/2} (1 - \zeta_p^{-i}) = \\ &= (-1)^{(p-1)/2} \prod_{i=1}^{(p-1)/2} \zeta_p^{-i} \cdot \prod_{i=1}^{(p-1)/2} (1 - \zeta_p^i)^2 = (-1)^{(p-1)/2} \zeta_p^s \alpha^2, \quad \alpha \in \mathbb{Q}(\zeta_p), \\ s &= -\left(1 + 2 + \dots + \frac{p-1}{2}\right) = -\frac{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)}{2} = -\frac{(p^2-1)}{8}. \end{aligned}$$

Si s es par, $s = 2n$, entonces $\zeta_p^{2n} = (\zeta_p^n)^2$ y $p = (-1)^{(p-1)/2} \beta^2$ con $\beta \in \mathbb{Q}(\zeta_p)$. Si s es impar, se tiene que $p + s = 2m$ es par y $\zeta_p^s = \zeta_p^{p+s} = (\zeta_p^m)^2$. En cualquier caso, existe $\gamma \in \mathbb{Q}(\zeta_p)$ tal que $(-1)^{(p-1)/2} p = \gamma^2$ y por lo tanto $\gamma = \sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}(\zeta_p)$.

Ahora bien, por unicidad del subcampo cuadrático, se tiene que

$$\mathbb{Q}\left(\sqrt{-(-1)^{\frac{p-1}{2}} p}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p+1}{2}} p}\right) \not\subseteq \mathbb{Q}(\zeta_p).$$

Además

$$\begin{aligned} \mathbb{Q}(\sqrt{p}, \sqrt{-p}) &= \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}, \sqrt{(-1)^{\frac{p+1}{2}} p}\right) = \mathbb{Q}\left(\zeta_4, \sqrt{(-1)^{\frac{p-1}{2}} p}\right) \\ &\subseteq \mathbb{Q}(\zeta_4, \zeta_p) = \mathbb{Q}(\zeta_{4p}). \end{aligned}$$

Para $p = 2$, se tiene que

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_8), \quad \mathbb{Q}(\sqrt{2}, \sqrt{-2}) \not\subseteq \mathbb{Q}(\zeta_4)$$

y de hecho

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(\zeta_4, \sqrt{2}) = \mathbb{Q}(\zeta_4, \sqrt{-2}) = \mathbb{Q}(\sqrt{2}, \sqrt{-2}) = \mathbb{Q}(\zeta_4, \sqrt{2}, \sqrt{-2}).$$

En general, si $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados, digamos $d = \pm p_1 \cdots p_r$, p_1, \dots, p_r primos distintos, entonces

$$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_4, \sqrt{p_1}, \dots, \sqrt{p_r}) \subseteq \mathbb{Q}(\zeta_8, \zeta_{p_1}, \dots, \zeta_{p_r}) \subseteq \mathbb{Q}(\zeta_{8p_1 \cdots p_r})$$

lo cual es una manera explícita, en este caso, del Teorema de Kronecker-Weber.

5.4. Anillos de enteros y unidades

Para $n \in \mathbb{N}$ se tiene que $\mathbb{Z}[\zeta_n] = \mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Una pregunta natural es si esto se cumple para todos los subcampos que hemos estudiado, es decir, si $M_b T_r = \mathbb{Q}(\mu_b, \delta_r)$, entonces, ¿es el anillo de enteros de $M_b T_r$ de la forma $\mathbb{Z}[\alpha]$ para algún α ?

Teorema 5.4.1. *El anillo de enteros de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ es $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Demostración. Sea $\alpha = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + \cdots + a_m(\zeta_n + \zeta_n^{-1})^m$ con $a_i \in \mathbb{Q}$ un entero de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Puesto que $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \varphi(n)/2$, se tiene que $m \leq (\varphi(n)/2) - 1$. Queremos probar que $a_i \in \mathbb{Z}$ con lo cual obtendremos que $\mathcal{O}_{\mathbb{Q}(\zeta_n)^+} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Puesto que la otra contención es inmediata, se seguirá la igualdad y el teorema.

Ahora bien, restando a ambos miembros de la igualdad anterior los términos tales que $a_i \in \mathbb{Z}$, en caso de ser falsa nuestra afirmación, podemos suponer que $a_m \notin \mathbb{Z}$.

Multiplicando a ambos miembros por ζ_n^m , obtenemos

$$\zeta_n^m \alpha = a_m + b_1 \zeta_n + \cdots + b_{2m-1} \zeta_n^{2m-1} + a_m \zeta_n^{2m}$$

el cual es un elemento de $\mathbb{Q}(\zeta_n)$ y además es un entero algebraico, es decir, $\zeta_n^m \alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. Además se tiene que $2m \leq 2\varphi(n) - 2 \leq \varphi(n) - 1$ y puesto que $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$ es una base entera de $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$, se sigue que $a_m \in \mathbb{Z}$, probando el resultado. \square

El Teorema 5.4.1 prueba que, en la notación del Teorema 5.3.4, si $c = 2$, $b = (p-1)/2$, $r = 0$, entonces siempre se tiene que el anillo de enteros de $\mathbb{Q}(\mu_{(p-1)/2})$ es $\mathbb{Z}[\mu_{(p-1)/2}]$. Sin embargo, para $b < (p-1)/2$, inclusive con $r = 0$, el resultado ya no sigue siendo cierto.

Ejemplo 5.4.2. Consideremos dos números primos distintos, p, q con $q > 2$ tales que si $f = o(p \bmod q)$, entonces $(q-1)/f > p$. Sea $E \subseteq \mathbb{Q}(\zeta_q)$ el subcampo de grado $\frac{q-1}{f}$ sobre \mathbb{Q} . Entonces p se descompone totalmente en la extensión E/\mathbb{Q} ya que p es no ramificado en $\mathbb{Q}(\zeta_q)$ y el grupo de descomposición de p es $\text{Gal}(\mathbb{Q}(\zeta_q)/E)$. Si el anillo de enteros \mathcal{O}_E de E fuese de la forma $\mathbb{Z}[\alpha]$ para algún α , entonces si $f(x) := \text{Irr}(\alpha, x, \mathbb{Q})$, tendríamos por el

Teorema de Kummer, Teorema 1.1.4, que $f(x)$ se descompone en en $\frac{q-1}{f}$ factores lineales mónicos distintos módulo p . Sin embargo, esto no es posible pues únicamente existen p factores lineales mónicos distintos módulo p , a saber, $x, x+1, \dots, x+(p-1)$ y por hipótesis tenemos $\frac{q-1}{f} > p$, $f < \frac{q-1}{p}$.

Notemos que en este ejemplo, $b = \frac{q-1}{f}$, $c = f$.

Observamos que debemos tener necesariamente que $c = f > 2$, y $\frac{q-1}{f} > p$, esto es, $2 < f < \frac{q-1}{p}$. Un ejemplo en que se cumple lo anterior es $p = 2$, $q = 31$. Se tiene que $2^5 = 32 \equiv 1 \pmod{31}$, $o(2 \pmod{31}) = 5$, es decir, $f = 5$ y $\frac{q-1}{f} = \frac{31-1}{5} = 6 > p = 2$.

Otro ejemplo es $p = 3$, $q = 1093$. Entonces $3^7 = 2187 \equiv 1 \pmod{1093}$ y $o(3 \pmod{1093}) = 7 = f$, $\frac{1093-1}{f} = \frac{1092}{7} = 156 > p = 3$. En otras palabras el campo de grado 156 sobre \mathbb{Q} contenido en $\mathbb{Q}(\zeta_{1093})$ no es de la forma $\mathbb{Z}[\alpha]$ para ningún α .

5.5. Teorema de reciprocidad cuadrática

Recordemos el *símbolo de Legendre*. Para dos números $n, p \in \mathbb{Z}$, con p primo y $p \nmid n$, sea $\left(\frac{n}{p}\right)$ el símbolo de Legendre, el cual está definido por:

$$\begin{aligned} \left(\frac{n}{p}\right) &= \begin{cases} 1 & \text{si } n \text{ es un residuo cuadrático mód } p \\ -1 & \text{si } n \text{ no es un residuo cuadrático mód } p \end{cases} = \\ &= \begin{cases} 1 & \text{si } \exists x \in \mathbb{Z} \text{ tal que } n \equiv x^2 \pmod{p} \\ -1 & \text{si } \nexists x \in \mathbb{Z} \text{ tal que } n \equiv x^2 \pmod{p} \end{cases} . \end{aligned}$$

Teorema 5.5.1 (Teorema de reciprocidad cuadrática). Sean p y q dos primos racionales impares distintos. Entonces

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} .$$

Demostración. Primero, sean $p \equiv 1 \pmod{4}$ y q arbitrario. Entonces

$$\left(\frac{p}{q}\right) = 1 \iff \text{existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv p \pmod{q} .$$

Escribamos $p = 1 + 4m$ para algún $m \in \mathbb{Z}$. Entonces

$$x^2 \equiv p \pmod{q} \iff x^2 - 1 \equiv 4m \pmod{q} .$$

Ahora bien, puesto que q es impar, 2 es invertible módulo q . Por tanto

$$x^2 - 1 \equiv 4m \pmod{q} \iff \frac{x+1}{2} \cdot \frac{x-1}{2} \equiv m \pmod{q} .$$

Sea $y = \frac{x+1}{2}$. Por tanto $y - 1 = \frac{x-1}{2}$. Entonces

$$\frac{x+1}{2} \cdot \frac{x-1}{2} \equiv m \pmod{q} \iff y(y-1) \equiv m \pmod{q}$$

lo cual es equivalente a que $y^2 - y - m = y^2 - y + \frac{1-p}{4} \equiv 0 \pmod{q}$.

Ahora sea $\alpha = \frac{1+\sqrt{p}}{2}$. Entonces $\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \mathbb{Z}[\alpha]$. Tenemos $(2\alpha - 1)^2 = p$. Por tanto $4\alpha^2 - 4\alpha + 1 = p$ lo cual equivale a $\alpha^2 - \alpha + \frac{1-p}{4} = 0$. Es decir

$$f(x) := \text{Irr}(\alpha, x, \mathbb{Q}) = x^2 - x + \frac{1-p}{4}.$$

Entonces q se descompone en $\mathbb{Q}(\sqrt{p})$ si y solamente si $f(x) \pmod{q}$ se factoriza como dos factores lineales. Esto último es equivalente a que $f(x)$ tenga raíces módulo q , esto es, si y solamente si $y^2 - y + \frac{1-p}{4} \equiv 0 \pmod{q}$ tiene solución.

En resumen, tenemos que $\left(\frac{p}{q}\right) = 1$ si y solamente si q se descompone en $\mathbb{Q}(\sqrt{p})$.

Por otro lado tenemos que q se descompone en $\mathbb{Q}(\sqrt{p})$ si y solamente si $\mathbb{Q}(\sqrt{p})$ está contenido en el campo de descomposición de q en $\mathbb{Q}(\zeta_p)$ y puesto que este último es el campo fijo bajo el automorfismo de Frobenius correspondiente a q , es decir a $\mathbb{Q}(\zeta_p)^{\langle \sigma_q \rangle}$, se tiene

$$q \text{ se descompone en } \mathbb{Q}(\sqrt{p}) \iff \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)^{\langle \sigma_q \rangle} \iff \sigma_q \text{ fija a } \mathbb{Q}(\sqrt{p}).$$

Ahora bien, σ_q está definido por $\sigma_q(\zeta_p) = \zeta_p^q$ y como la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es una extensión cíclica, se tiene la existencia de un único campo de grado h sobre \mathbb{Q} para cada divisor h de $p-1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$. Si definimos $f := o(\sigma_q) = o(q \pmod{p})$, se tiene que

$$\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)^{\langle \sigma_q \rangle} \iff f \mid \frac{\varphi(p)}{2} = \frac{p-1}{2} \iff q^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Sea a un generador módulo p , esto es, $o(a \pmod{p}) = p-1$. Sea $a^t \equiv q \pmod{p}$. Entonces $a^{t\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ lo cual equivale a que $p-1 \mid t\frac{p-1}{2}$, esto es, $t = 2s$ es par y por tanto si $b = a^s$ se tiene $b^2 = a^{2s} = a^t \equiv q \pmod{p}$, es decir la ecuación $z^2 \equiv q \pmod{p}$ es soluble. Esto último equivale a que $\left(\frac{q}{p}\right) = 1$.

En resumen, hemos probado que si $p \equiv 1 \pmod{4}$, entonces para cualquier primo impar q ,

$$\left(\frac{p}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1.$$

Por tanto $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ y el resultado se sigue en este caso. Por simetría lo mismo tenemos para $q \equiv 1 \pmod{4}$ y p cualquier primo impar.

Ahora sean p y q dos primos diferentes congruentes con 3 módulo 4. Primero notemos que $x^2 \equiv -1 \pmod{q}$ no es soluble pues si lo fuese $x^4 \equiv 1 \pmod{q}$ y por tanto $o(x \pmod{q}) = 4$ por lo que $4 \mid q-1 = o(U_q)$, lo que contradice que $q \equiv 3 \pmod{4}$.

Por tanto tenemos que $x^2 \equiv a \pmod{q}$ es soluble si y solamente si $y^2 \equiv -a \pmod{q}$ no es soluble pues si ambas lo fuesen se tendría que $(x/y)^2 \equiv (a/-a) \equiv -1 \pmod{q}$.

De esta forma obtenemos que $\left(\frac{-p}{q}\right) = -\left(\frac{p}{q}\right)$. Ahora bien, general tenemos $\left(\frac{p}{-q}\right) = \left(\frac{p}{q}\right)$. Se tiene $-p \equiv 1 \pmod{4}$ de donde, por la primera parte, obtenemos

$$-\left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right) = \left(\frac{q}{-p}\right) = \left(\frac{q}{p}\right),$$

es decir $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = -1 = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$. □

Caracteres de Dirichlet

6.1. Teoría de caracteres

Primeramente recordemos los resultados básicos de la teoría de caracteres.

Definición 6.1.1. Sea G un grupo cualquiera. El *grupo de caracteres* de G se define como el grupo de homomorfismos de G en el grupo multiplicativo de los complejos:

$$\text{Hom}(G, \mathbb{C}^*) = \{f: G \rightarrow \mathbb{C}^* \mid f \text{ es homomorfismo de grupos}\}.$$

Cuando G es finito, si $n = |G|$, entonces si f es un caracter y $g \in G$, entonces $1 = f(e) = f(g^n) = f(g)^n$, es decir, $f(g) \in W_n$ y podemos definir $\text{Hom}(G, W_n)$ como el grupo de caracteres de G .

Si f es un caracter y G es un grupo topológico tal que para todo $g \in G$, $f(g)$ es de orden finito, es decir, para cada $g \in G$, existe $n_g \in \mathbb{N}$ tal que $f(g)^{n_g} = 1$, entonces $f(g) \in W_{n_g}$. Sea $R := \mathbb{Q}/\mathbb{Z} = \bigcup_{n=1}^{\infty} W_n \subseteq \mathbb{C}^*$ con la topología discreta. Entonces definimos

$$\hat{G} := \text{Hom}(G, R) \subseteq \text{Hom}(G, \mathbb{C}^*)$$

donde $\text{Hom}(G, R) := \{f: G \rightarrow R \mid f \text{ es continuo}\}$.

En general estaremos interesados en \hat{G} y en general si G es un grupo finito, $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. En este caso G tiene la topología discreta y todos los homomorfismos son automáticamente continuos.

Ejemplo 6.1.2. Sea $f \in \hat{\mathbb{Z}}$. Entonces f está completamente determinado por $f(1) \in R$. Sea

$$\begin{aligned} \varphi: \hat{\mathbb{Z}} &\longrightarrow R \\ f &\longmapsto f(1). \end{aligned}$$

Entonces φ es un isomorfismo de grupos y $\hat{\mathbb{Z}} \cong R$. Observemos que en este ejemplo, $\hat{\mathbb{Z}}$ no denota al anillo de Prüfer (Ejemplo 2.1.15).

Ejemplo 6.1.3. Sea \mathbb{Z}_p el anillo de los enteros p -ádicos (Ejemplos 2.1.15 (3)) y sea \mathbb{Q}_p el campo de los números p -ádicos, $\mathbb{Q}_p = \text{coc } \mathbb{Z}_p$. Sea $f \in \hat{\mathbb{Z}}_p$. Si $g \in \mathbb{Z}_p$, $f(ng) = nf(g) = 0 \in R$ para alguna $n \in \mathbb{N}$. Ahora, si $n = p^m s$ con $(s, p) = 1$, s es invertible en \mathbb{Z}_p y existe $t \in \mathbb{Z}_p$ tal que $st = 1$. Como \mathbb{Z}_p es la cerradura de \mathbb{Z} en la topología p -ádica, existe una sucesión $\{t_i\}_{i=1}^\infty \subseteq \mathbb{Z}$ tal que $\lim_{i \rightarrow \infty} t_i = t$ en la topología p -ádica. Puesto que f es continua,

$$\begin{aligned} f(p^m g) &= f(p^m stg) = \lim_{i \rightarrow \infty} f(st_i p^m g) = \\ &= \lim_{i \rightarrow \infty} t_i f(sp^m g) = \lim_{i \rightarrow \infty} t_i f(ng) = \lim_{i \rightarrow \infty} 0 = 0. \end{aligned}$$

Por tanto, $f(p^m g) = p^m f(g) = 0$, es decir, $f(\hat{\mathbb{Z}}_p) = R(p) = (\mathbb{Q}/\mathbb{Z})(p) \cong \mathbb{Q}_p/\mathbb{Z}_p =: R_p$.

Ahora bien, por continuidad, f está totalmente determinado por $f(1)$ pues si $x \in \mathbb{Z}_p$, existe una sucesión $\{x_n\}_{n=1}^\infty \subseteq \mathbb{Z}$ tal que $x_n \xrightarrow{n \rightarrow \infty} x$ en la topología p -ádica y $f(x) = \lim_{n \rightarrow \infty} (f(x_n)) = \lim_{n \rightarrow \infty} x_n f(1) = x f(1)$.

Por tanto

$$\begin{aligned} \hat{\mathbb{Z}}_p &\longrightarrow R_p = \mathbb{Q}_p/\mathbb{Z}_p \\ f &\longmapsto f(1) \end{aligned}$$

es un isomorfismo de grupos y $\hat{\mathbb{Z}}_p \cong R_p$.

Proposición 6.1.4. Si G es un grupo cíclico finito, se tiene $\hat{G} \cong G$.

Demostración. Sea $G \cong C_m$ para alguna m y sea a un generador de G . Entonces cualquier $f \in \hat{G}$ está completamente determinado por $f(a)$ y $f(a)^m = f(a^m) = f(e) = 1 \in \mathbb{C}^*$, es decir, $f(a) \in W_m$. Por lo tanto, $\hat{G} = \text{Hom}(G, W_m)$. Finalmente, tenemos que $\varphi: \hat{G} \rightarrow W_m$, $a \mapsto f(a)$ es un isomorfismo de grupos. \square

Observación 6.1.5. El isomorfismo de la Proposición 6.1.4 no es canónico pues depende del generador a seleccionado.

Teorema 6.1.6. Si G es un grupo finito, entonces $\hat{G} \cong G/G'$ donde G' denota al subgrupo conmutador. En particular, si G es un grupo abeliano finito, entonces $\hat{G} \cong G$.

Demostración. Si $f \in \hat{G}$, puesto que, ya sea R o \mathbb{C}^* son abelianos, se tiene que $G' \subseteq \text{núc } f$ y por lo tanto f se factoriza de manera única

$$\begin{array}{ccc} G & \xrightarrow{f} & R \\ & \searrow \pi & \nearrow \tilde{f} \\ & G/G' & \end{array}$$

donde $\pi: G \rightarrow G/G'$ es la proyección natural y $f = \tilde{f} \circ \pi$.

Puesto que G/G' es un grupo abeliano finito y se tiene $\hat{G} = \widehat{G/G'}$, para terminar la demostración, basta probar que $G \cong \hat{G}$ para un grupo abeliano finito.

Sea $G \cong C_{n_1} \times \cdots \times C_{n_r}$ un grupo abeliano finito cualquiera. En general, si $G = H_1 \times H_2$, la función

$$\begin{aligned} \hat{G} &\longrightarrow \hat{H}_1 \times \hat{H}_2 \\ f &\longmapsto (f|_{H_1}, f|_{H_2}) \end{aligned}$$

es un isomorfismo de grupos. Por lo tanto, por la Proposición 6.1.4

$$\hat{G} \cong \hat{C}_{n_1} \times \cdots \times \hat{C}_{n_r} \cong C_{n_1} \times \cdots \times C_{n_r} \cong G. \quad \square$$

Observación 6.1.7. El Teorema 6.1.6 no es válido para grupos abelianos infinitos, por ejemplo, $\hat{\mathbb{Z}} \cong R \not\cong \mathbb{Z}$ (ver Ejemplo 6.1.2).

Definición 6.1.8. Sean G, H grupos topológicos cualesquiera. Un *apareamiento* es una función bilineal continua $\varphi: G \times H \rightarrow \mathbb{C}^*$, es decir,

$$\begin{aligned} \varphi(xy, z) &= \varphi(x, z)\varphi(y, z), \\ \varphi(u, vw) &= \varphi(u, v)\varphi(u, w), \end{aligned}$$

para cualesquiera $x, y, u \in G$ y $z, v, w \in H$.

Un apareamiento se llama *no degenerado* si

$$\varphi(x, y) = 1 \quad \forall y \in H \implies x \in G' \quad \text{y} \quad \varphi(u, v) = 1 \quad \forall u \in G \implies v \in H'.$$

Teorema 6.1.9. Si G y H son grupos finitos y existe un apareamiento no degenerado $\varphi: G \times H \rightarrow \mathbb{C}^*$, entonces

$$\begin{aligned} \psi: G &\longrightarrow \hat{H} & \theta: H &\longrightarrow \hat{G} \\ g &\longmapsto \varphi(g, -) & h &\longmapsto \varphi(-, h) \end{aligned}$$

son epimorfismos de grupos y $\text{nuc } \psi = G', \text{nuc } \theta = H'$. En particular, $G/G' \cong \hat{H}; H/H' \cong \hat{G}$ y $G/G' \cong H/H'$. Finalmente si G y H son grupos abelianos, entonces $G \cong H$.

Demostración. Si $g \in G$, sea $\psi_g: H \rightarrow \mathbb{C}^*$ dada por $\psi_g(h) = \varphi(g, h)$. Entonces ψ_g es un homomorfismo y por tanto $\psi_g \in \hat{H}$.

Además, si $g, g_1 \in G$, se tiene $\psi_{gg_1}(h) = \varphi(gg_1, h) = \varphi(g, h)\varphi(g_1, h) = \psi_g(h)\psi_{g_1}(h)$ para toda $h \in H$ por lo que $\psi_{gg_1} = \psi_g\psi_{g_1}$ y

$$\begin{aligned} \psi: G &\rightarrow \hat{H} \\ g &\mapsto \psi_g = \varphi(g, -) \end{aligned}$$

es un homomorfismo de grupos. Si $g \in G'$, puesto que \mathbb{C}^* es abeliano, $\psi_g = 1$ y por lo tanto $g \in \text{nuc } \psi$. Se sigue que $G' \subseteq \text{nuc } \psi$. Ahora bien, si $g \in \text{nuc } \psi$, por ser φ no degenerada se sigue que $g \in G'$ y por lo tanto $G' = \text{nuc } \psi$.

Bajo ψ tenemos que $G/G' \subseteq \hat{H} \cong H/H'$. De manera análoga obtenemos $H/H' \subseteq \hat{G} \cong G/G'$. El resultado se sigue. \square

Sea G un grupo abeliano finito y consideremos el mapeo

$$\varphi = \langle \cdot, \cdot \rangle: G \times \hat{G} \rightarrow \mathbb{C}^*, \quad \langle \cdot, \cdot \rangle(g, \psi) = \langle \chi, g \rangle := \chi(g).$$

Entonces

$$\langle \chi_1 \chi_2, g \rangle = (\chi_1 \chi_2)(g) = \chi_1(g) \chi_2(g) = \langle \chi, g \rangle \langle \chi_2, g \rangle$$

y

$$\langle \chi, gh \rangle = \chi(gh) = \chi(g) \chi(h) = \langle \chi, g \rangle \langle \chi, h \rangle,$$

es decir, φ es un apareamiento.

Si $\langle g, \chi \rangle = 1$ para toda $\chi \in \hat{G}$, entonces $\chi(g) = 1$ para toda $\chi \in \hat{G}$. Sea $H = \langle g \rangle$. Entonces dado $\chi \in \hat{G}$, χ se puede factorizar de manera única:

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \nearrow \tilde{\chi} \\ & G/H & \end{array} \quad \tilde{\chi} \circ \pi = \chi$$

y por tanto $\begin{array}{c} \hat{G} \rightarrow \widehat{G/H} \\ \chi \mapsto \tilde{\chi} \end{array}$ es un monomorfismo. Por lo tanto $|G| = |\hat{G}| \leq |(\widehat{G/H})| = |G/H| \leq |G|$, lo cual implica que $|H| = 1$ y $g = e$.

Recíprocamente, si $\langle g, \chi \rangle = 1$ para toda $g \in G$, entonces $\chi(g) = 1$ para toda $g \in G$ lo cual, por definición, nos dice que $\chi = 1$.

Esto prueba que φ es un mapeo no degenerado. En particular, cuando G es

un grupo abeliano finito, $G \cong \hat{\hat{G}}$ de manera canónica. Es decir, $\begin{array}{c} \theta: G \rightarrow \hat{\hat{G}} \\ g \mapsto \hat{g} \end{array}$

definido por $\hat{g}: \hat{G} \rightarrow \mathbb{C}^*$, $\hat{g}(\chi) = \chi(g)$, es un isomorfismo de grupos.

Definición 6.1.10. Sean G un grupo abeliano finito y $\langle \cdot, \cdot \rangle: G \times \hat{G} \rightarrow \mathbb{C}^*$ el mapeo bilineal $\langle g, \chi \rangle = \chi(g)$. Sea $H < G$. Definimos el *ortogonal* de H por

$$H^\perp := \langle \chi \in \hat{G} \mid \chi(h) = 1 \ \forall h \in H \rangle.$$

Proposición 6.1.11. Se tiene $H^\perp \cong \widehat{(G/H)}$.

Demostración. Si $\chi \in H^\perp$, χ se factoriza de manera única

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \nearrow \tilde{\chi} \\ & G/H & \end{array}$$

con $\tilde{\chi} \in (\widehat{G/H})$ y viceversa, si $\tilde{\chi} \in (\widehat{G/H})$, entonces $\tilde{\chi}$ se puede levantar a un elemento $\chi \in \hat{G}$: $\chi(g) := \tilde{\chi}(gH)$. Por lo tanto $\chi \rightarrow \tilde{\chi}$ es un isomorfismo entre H^\perp y $(\widehat{G/H})$. \square

Ahora bien, si consideramos el mapeo restricción

$$\begin{aligned} \text{rest}: \hat{G} &\longrightarrow \hat{H} \\ \chi &\longmapsto \chi|_H \end{aligned}$$

se tiene que $\text{nuc}(\text{rest}) = H^\perp$ y por lo tanto se tiene $\hat{G}/H^\perp \subseteq \hat{H}$.

Proposición 6.1.12. *Se tiene $\hat{H} \cong \hat{G}/H^\perp$.*

Demostración. Hemos obtenido $\hat{G}/H^\perp \subseteq \hat{H}$ y

$$|\hat{G}/H^\perp| = \frac{|\hat{G}|}{|H^\perp|} = \frac{|G|}{|(\widehat{G/H})|} = \frac{|G|}{|G/H|} = |H| = |\hat{H}|$$

de donde se sigue la igualdad. \square .

Identificamos G con \hat{G} como antes. Con esta identificación, tenemos:

Proposición 6.1.13. $(H^\perp)^\perp = H^{\perp\perp} = H$.

Demostración. Por la Proposición 6.1.11 $(H^\perp)^\perp \cong (\widehat{\hat{G}/H^\perp})$ y por lo tanto

$$|H^{\perp\perp}| = |(\widehat{\hat{G}/H^\perp})| = |\hat{G}/H^\perp| = \frac{|\hat{G}|}{|H^\perp|} = \frac{|G|}{|(\widehat{G/H})|} = \frac{|G|}{|G/H|} = |H|.$$

Por otro lado, si $h \in H$, entonces $h: \chi \rightarrow \chi(h)$ satisface que $h(H^\perp) = 1$ por definición y por tanto $h \in (H^\perp)^\perp$. Es decir, $H \subseteq (H^\perp)^\perp$ y como tiene la misma cardinalidad se sigue que $H = (H^\perp)^\perp = H^{\perp\perp}$. \square

Hay varios resultados elementales que son de gran utilidad y que probaremos a continuación.

Proposición 6.1.14. *Sea $\chi \in \hat{G}$. Si $\chi \neq 1$, entonces $\sum_{g \in G} \chi(g) = 0$. Si $\chi = 1$, entonces $\sum_{g \in G} \chi(g) = |G|$.*

Demostración. Si χ es trivial, esto es, $\chi = 1$, es inmediato que $\sum_{g \in G} \chi(g) = |G|$. Ahora, si $\chi \neq 1$, existe un elemento $h \in G$ tal que $\chi(h) \neq 1$. Sea $t = \sum_{g \in G} \chi(g) \in \mathbb{C}$. Entonces

$$\chi(h)t = \chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(h)\chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g) = t.$$

Por tanto $t(\chi(h) - 1) = 0$. Puesto que $\chi(h) \neq 1$ se sigue que $t = 0$. \square

Proposición 6.1.15. Sean G un grupo abeliano finito y $H < G$. Entonces G tiene un subgrupo isomorfo a G/H .

Demostración. Una prueba directa de este resultado es simplemente el teorema de estructura de los grupos abelianos finitamente generados. Ahora, usando la teoría de caracteres, tenemos

$$G/H \cong (\widehat{G/H}) \cong H^\perp \subseteq \hat{G} \cong G. \quad \square$$

Observación 6.1.16. La segunda demostración de la Proposición 6.1.15, nos indica que el mapeo entre redes

$$\begin{aligned} \mathcal{A} = \{H \mid H < G\} &\longrightarrow \mathcal{B} = \{G/H \mid H < G\} \\ H &\longmapsto G/H \end{aligned}$$

entre los subgrupos de un grupo abeliano y sus grupos cocientes, es biyectiva y que la red de subgrupos \mathcal{A} de G es simétrica.

6.2. Caracteres de Dirichlet

Aplicamos toda la teoría de caracteres al caso especial del grupo $U_n \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ el cual es un grupo abeliano finito.

Definición 6.2.1. Un *caracter de Dirichlet* es un elemento de \hat{U}_n para algún $n \in \mathbb{N}$. Explícitamente, un caracter de Dirichlet χ es un homomorfismo de grupos $\chi: U_n \rightarrow \mathbb{C}^*$.

Ahora bien, si $\chi \in \hat{U}_n$ y $n|m$, entonces χ se puede considerar un elemento \hat{U}_m de la siguiente forma. Sea $\varphi_{m,n}: U_m \rightarrow U_n$ la proyección natural: $\varphi_{m,n}(x \bmod m) := x \bmod n$ y sea $\tilde{\chi} := \chi \circ \varphi_{m,n}$:

$$\begin{array}{ccc} U_m & \xrightarrow{\tilde{\chi}} & \mathbb{C}^* \\ & \searrow \varphi_{m,n} & \nearrow \chi \\ & U_n & \end{array}$$

En cierta forma χ y $\tilde{\chi}$ son el mismo mapeo y χ puede considerarse módulo n o módulo m . Recíprocamente, si existe $f|n$ y $\chi': U_f \rightarrow \mathbb{C}^*$ tal que $\chi = \chi' \circ \varphi_{n,f}$, entonces también podemos definir χ módulo f usando χ' en lugar de χ .

Observación 6.2.2. Para $n, m \in \mathbb{N}$ tales que $m|n$, se tiene que el homomorfismo $\varphi_{n,m}: U_n \rightarrow U_m$ es suprayectivo. Esto se sigue del epimorfismo natural de anillos $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ cuyos grupos de unidades son U_n y U_m respectivamente. Una demostración directa sería la siguiente: sea $a \in \mathbb{Z}$ tal que $\text{mcd}(a, m) = 1$. Queremos hallar $c \in \mathbb{Z}$ tal que $\text{mcd}(c, n) = 1$ y $\varphi_{n,m}(c \bmod n) = a \bmod m$,

esto es, debemos hallar $c \in \mathbb{Z}$ tal que $\text{mcd}(c, n) = 1$ y $c \equiv a \pmod{m}$. Sea $n = rm$ y escribimos

$$r = p_1^{\alpha_1} \cdots p_t^{\alpha_t} q_1^{\beta_1} \cdots q_s^{\beta_s} u_1^{\gamma_1} \cdots u_\ell^{\gamma_\ell}$$

con $p_1, \dots, p_t, q_1, \dots, q_s, u_1, \dots, u_\ell$ primos distintos y tales que

$$u_1, \dots, u_\ell \mid m, \quad p_1, \dots, p_t, q_1, \dots, q_s \nmid m, \quad q_1, \dots, q_s \mid a, \quad p_1, \dots, p_t \nmid a.$$

Sea $c := a + xm$ con $x := p_1 \cdots p_t$. Entonces $c \equiv a \pmod{m}$ y en particular $\text{mcd}(c, m) = 1$. Por lo tanto $u_1, \dots, u_\ell \nmid c$. Ahora bien, $q_i \mid a$ y $q_i \nmid xm$ para $1 \leq i \leq s$ de donde se sigue que $q_i \nmid c$. Finalmente $p_j \mid x$ y $p_j \nmid a$ por lo que $p_j \nmid c$, $1 \leq j \leq t$.

De esta forma obtenemos que $\text{mcd}(c, r) = 1$ y por tanto $\text{mcd}(c, rm) = \text{mcd}(c, n) = 1$ que es lo que queríamos obtener.

Definición 6.2.3. Dado un caracter de Dirichlet χ el mínimo número natural f tal que χ puede ser definido módulo f se llama el *conductor* de χ y se denota por f_χ .

Más precisamente, definimos para $a, b \in \mathbb{N}$ el siguiente orden

$$a \leq_* b \iff a \mid b.$$

Se tiene que \leq_* es un orden parcial. Se definen *los conductores* del caracter χ definido módulo n como los elementos minimales bajo el orden \leq_* del conjunto $\{m \leq_* n \mid \chi \text{ puede ser definido módulo } m\}$. Veremos que hay un único elemento mínimo de este conjunto y este será el conductor de χ (ver Observación 6.2.8 y Teorema 6.2.9).

Observación 6.2.4. Dado χ un caracter de Dirichlet definido módulo n y si $m \mid n$, entonces χ puede definirse módulo m , es decir, existe $\tilde{\chi}: U_m \rightarrow \mathbb{C}^*$ tal que $\chi = \tilde{\chi} \circ \varphi_{n,m}$, si y solamente si para cualesquiera $a, b \in \mathbb{Z}$ con $\text{mcd}(a, n) = \text{mcd}(b, n) = 1$ y tales que $a \equiv b \pmod{m}$, se tiene $\chi(a \pmod{n}) = \chi(b \pmod{n})$ (en este caso se define $\tilde{\chi}(c \pmod{m}) := \chi(a \pmod{n})$ donde $\text{mcd}(a, n) = 1$ y $a \equiv c \pmod{m}$).

Ejemplo 6.2.5. Consideremos $n = 8$, $U_8 = \{1, 3, 5, 7\} \cong C_2 \times C_2$. Sea $\chi: U_8 \rightarrow \mathbb{C}^*$ definido por $\chi(1) = \chi(5) = 1; \chi(3) = \chi(7) = -1$. Puesto que $\chi(1) = \chi(1+4) = \chi(5)$ y $\chi(3) = \chi(3+4) = \chi(7)$ se tiene que χ puede definirse módulo 4. Se tiene que $U_4 = \{\pm 1\}$ entonces $\chi': U_4 \rightarrow \mathbb{C}^*$ dado por $\chi'(1) = 1$ y $\chi'(-1) = -1$ satisface que

$$\begin{aligned} \chi'(1) &= \chi \circ \varphi_{8,4}(1) = \chi(1) = \chi(5) = 1; \\ \chi'(-1) &= \chi \circ \varphi_{8,4}(-1) = \chi(3) = \chi(7) = -1. \end{aligned}$$

Además χ no puede definirse módulo 2 pues $U_2 = \{1\}$ y $\chi(1) \neq \chi(-1)$, $1 \equiv -1 \pmod{2}$. Por lo tanto $f_\chi = 4$.

Ahora consideremos $\sigma \in U_8$ dado por $\sigma(1) = \sigma(3) = 1$ y $\sigma(5) = \sigma(7) = -1$. Notemos que $\sigma(1) \neq \sigma(5)$ y $1 \equiv 5 \pmod{4}$ por lo que σ no puede definirse módulo 4 y por lo tanto $f_\sigma = 8$.

Ejemplo 6.2.6. Consideremos $U_{10} = \{1, 3, 7, 9\}$. Se tiene que $U_5 = \{1, 2, 3, 4\}$ y $U_5 \cong U_{10}$ con $\varphi_{10,5}: U_{10} \rightarrow U_5$, $\varphi_{10,5}(x \pmod{10}) = x \pmod{5}$. Entonces $\varphi_{10,5}(1) = 1, \varphi_{10,5}(3) = 3, \varphi_{10,5}(7) = 2, \varphi_{10,5}(9) = \varphi_{10,5}(-1) = -1 = 4$.

Si $\chi \in U_{10}$ entonces χ puede automáticamente definirse módulo 5 con $\chi' = \chi \circ \varphi_{10,5}$ y por lo tanto $f_\chi = 1$ o 5. Además $f_\chi = 1 \iff \chi(x) = 1 \forall x \in U_5$.

Por ejemplo, si $\chi(1) = 1, \chi(3) = \chi(7) = -1, \chi(-1) = \chi(9) = -1$, entonces $f_\chi = 5$. Similarmente, si $\sigma(3) = \zeta_4, \sigma(7) = \zeta_4^3, \sigma(1) = 1 = \zeta_4^0$ y $\sigma(9) = \zeta_4^{-1}$, entonces $f_\sigma = 5$.

Ejemplo 6.2.7. Si p es un número primo impar y $\chi \in U_p$, entonces si $\chi \neq 1$ necesariamente $f_\chi = p$. Si $\sigma \in U_{p^m}$ con $m \in \mathbb{N}$ y en caso de que p sea par, tomamos $m \geq 2$, entonces $f_\sigma = p^t$ para algún $0 \leq t \leq m$.

Observación 6.2.8. Si $\chi: U_n \rightarrow \mathbb{C}^*$ es un caracter de Dirichlet, el conductor de χ se definió como un número minimal f_χ tal que $\chi = \chi' \circ \varphi_{n,f_\chi}$ donde φ_{n,f_χ} donde φ_{n,f_χ} es el epimorfismo natural

$$\begin{aligned} \varphi_{n,f_\chi}: U_n &\longrightarrow U_{f_\chi} \\ x \pmod{n} &\longmapsto x \pmod{f_\chi}. \end{aligned}$$

Es decir el conductor f_χ de χ , en caso de existir, necesariamente divide a n . Aquí mencionamos que en caso de existir, lo cual es obvio si tomamos al pie de la letra la definición, es decir, f_χ es mínimo con $f_\chi | n$. Sin embargo, si pensamos la minimalidad en términos de divisibilidad (por ejemplo 2 y 3 son minimales dividiendo a 24), ya no es tan obvio que f_χ exista.

Para precisar, digamos que tenemos χ un caracter módulo 21 y que χ se puede definir módulo 3 y también 7 y que χ no es trivial.

Aunque por definición, $f_\chi = 3, 7$ también es minimal en el sentido de divisibilidad y por que no pensar que χ tiene dos conductores: 3 y 7.

En seguida veremos que esto no es posible y nuestra definición de f_χ quedará dado sin ambigüedad alguna.

Teorema 6.2.9 (Existencia del conductor). Sea $\chi: U_n \rightarrow \mathbb{C}^*$ un caracter de Dirichlet y sean $a|n, b|n$ tales que $\chi = \chi_a \circ \varphi_{n,a}$ y $\chi = \chi_b \circ \varphi_{n,b}$:

$$\begin{array}{ccc} U_n & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{n,a} \quad \nearrow \chi_a & \\ & U_a & \end{array} \quad \begin{array}{ccc} U_n & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{n,b} \quad \nearrow \chi_b & \\ & U_b & \end{array}$$

Sea $c := \text{mcd}(a, b)$. Entonces χ puede definirse módulo c . En particular, si a y b son dos conductores de χ , en el sentido de que no existen $x|a, y|b$ tales que χ pueda ser definido módulo x o módulo y , entonces $a = b$.

Demostración. Sea d el producto de todos los números primos p que dividen a n pero que no dividen a b . Entonces $c = \text{mcd}(da, b)$ pues si $\beta = \text{mcd}(da, b)$, como $c|a$ y $c|b$, entonces $c|da$ y $c|b$ por lo que $c|\beta$. Por otro lado existen $t, s, r, l \in \mathbb{Z}$ tales que $td + sb = 1$; $ra + lb = c$, por lo que al multiplicar ambas igualdades obtenemos

$$c = (tr)(ad) + (tdl + ras + slb)b$$

lo cual implica que $\beta|c$ y que $\beta = c$.

Para ver que χ puede ser definido módulo c , debemos probar que si $\text{mcd}(x, n) = 1$, $\text{mcd}(y, n) = 1$ y $x \equiv y \pmod{c}$, entonces $\chi(x) = \chi(y)$. Por el Teorema Chino del Residuo, existe $\alpha \in \mathbb{Z}$ tal que $\alpha \equiv x \pmod{da}$ y $\alpha \equiv y \pmod{b}$. De hecho, si $x = y + lc$ y sea $\varepsilon da + \delta b = c$, por lo que $l\varepsilon da + l\delta b = lc = x - y$. Entonces $\alpha := x - l\varepsilon da = y + l\delta b$.

Veremos primero que $\text{mcd}(\alpha, n) = 1$. Supongamos que p es un número primo tal que $p|\alpha$ y $p|n$. Se tiene que $p \nmid b$ pues en caso de que $p|b$ y debido a que $\alpha = y + mb$, entonces se tendría que $p|y$ y por tanto $p|\text{mcd}(y, n) = 1$ lo cual es absurdo. Así, $p \nmid b$.

Ahora bien, puesto que $p|n$, entonces $p|d$ por lo que $p|da$ y $p|\alpha$ lo cual implica que $p|x$ pero en ese caso tendríamos que $p|\text{mcd}(x, n) = 1$ lo cual nuevamente es absurdo.

En resumen, tenemos que $\text{mcd}(\alpha, n) = 1$. Se tiene

$$\begin{aligned}\chi(\alpha) &= \chi_a \circ \varphi_{n,a}(\alpha) = \chi_a \circ \varphi_{n,a}(x) = \chi(x), \\ \chi(\alpha) &= \chi_b \circ \varphi_{n,b}(\alpha) = \chi_b \circ \varphi_{n,b}(y) = \chi(y).\end{aligned}$$

Por tanto $\chi(\alpha) = \chi(x) = \chi(y)$ y χ puede ser definido módulo c .

$$\begin{array}{ccc} U_n & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{n,c} & \nearrow \chi_c \\ & U_c & \end{array}$$

Finalmente, si a y b son dos conductores de χ , entonces χ se puede definir módulo $c := \text{mcd}(a, b)$ y $c|a$, $c|b$. Por minimalidad de a y b se sigue que $a = c = b$. \square

Observación 6.2.10. Si $n = 1$, $U_1 = \{1\}$, $\chi: U_1 \rightarrow \mathbb{C}^*$, $1 \mapsto 1$ es único caracter módulo 1 y χ es el *caracter trivial*. Para toda $m \in \mathbb{N}$,

$$\begin{array}{ccc} U_m & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{m,1} & \nearrow \tilde{\chi} \\ & U_1 & \end{array} \quad \varphi_{m,1}(a) = 1 \text{ y } \tilde{\chi}(x) = 1 \text{ para toda } x \in U_m. \text{ Es decir,}$$

para toda m , $\tilde{\chi}$ es el caracter trivial y es el único caracter de conductor 1.

Observación 6.2.11. Sea $n \in \mathbb{N}$ impar. Entonces

$$\begin{aligned}\varphi_{2n,n}: U_{2n} &\longrightarrow U_n, \\ a \bmod 2n &\longmapsto a \bmod n.\end{aligned}$$

es un isomorfismo. Por lo tanto si χ es cualquier caracter módulo $2n$, χ puede definirse módulo n . $U_{2n} \xrightarrow{\chi} \mathbb{C}^*$ con $\tilde{\chi} := \chi \circ \varphi_{2n,n}^{-1}$.

$$\begin{array}{ccc} U_{2n} & \xrightarrow{\chi} & \mathbb{C}^* \\ \searrow \varphi_{2n,n} & & \nearrow \tilde{\chi} \\ & U_n & \end{array}$$

En particular no pueden existir caracteres con conductor $2n$ con n impar y en especial no hay caracteres de conductor 2.

Proposición 6.2.12. Sean χ, φ dos caracteres de Dirichlet de conductores f_χ y f_φ . Supongamos que existe $n \in \mathbb{N}$ tal que $f_\chi | n$ y $f_\varphi | n$ y tales que χ y φ son iguales módulo n , es decir, $\chi, \varphi: U_n \rightarrow \mathbb{C}^*$ satisfacen $\chi(a \bmod n) = \varphi(a \bmod n)$ para toda $\text{mcd}(a, n) = 1$. Entonces $\chi = \varphi$, es decir, $f_\chi = f_\varphi = f$ y $\chi = \varphi \bmod f$.

Demostración. Consideremos

$$\begin{array}{ccc} U_n & \xrightarrow{\varphi_{n, f_\chi = \pi}} & U_{f_\chi} \\ \searrow \chi & & \nearrow \tilde{\chi} \\ & \mathbb{C}^* & \end{array} \quad \tilde{\chi} \circ \pi = \chi = \varphi.$$

Por tanto $\tilde{\varphi} \circ \pi = \chi = \varphi$, es decir φ se puede definir módulo f_χ y en particular $f_\varphi | f_\chi$. Por simetría $f_\chi | f_\varphi$ y $f_\varphi = f_\chi$. Por lo tanto φ y χ son el mismo caracter módulo $f = f_\varphi = f_\chi$. \square

Con lo visto hasta ahora, es claro que el elemento $J \sim -1$ en el grupo de Galois $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U_n$ juega un papel importante en nuestra teoría. Baste decir que $K^J = K \iff K \subseteq \mathbb{R}$.

Definición 6.2.13. Sea $\chi: U_n \rightarrow \mathbb{C}^*$ un caracter de Dirichlet módulo n . Entonces χ se llama *par* si $\chi(-1) = 1$ e *impar* si $\chi(-1) = -1$ (notemos que $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$ por lo que necesariamente $\chi(-1) \in \{\pm 1\}$).

Puesto que un caracter de Dirichlet puede ser definido módulo muchos $n \in \mathbb{N}$, es conveniente fijar, en algunas ocasiones, el número n .

Definición 6.2.14. Si un caracter χ está definido módulo su conductor f_χ , χ se llama *primitivo*.

Muchas veces es conveniente definir $\chi(a)$ para $a \in \mathbb{Z}$ para un caracter de Dirichlet.

Definición 6.2.15. Dado un caracter de Dirichlet χ , definimos $\chi(a) = 0$ para $a \in \mathbb{Z}$ con $\text{mcd}(a, f_\chi) \neq 1$.

De esta forma podemos considerar $\chi: \mathbb{Z} \rightarrow \mathbb{C}^*$. Notemos que es importante fijar f_χ y no solo considerar χ módulo n pues de esta forma $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ no estaría unívocamente determinado.

Por ejemplo, si χ está dado por $\chi: U_3 \rightarrow \mathbb{C}$, $\chi(1) = 1, \chi(2) = -1$. Si consideramos χ módulo 12, $\chi: U_{12} \rightarrow \mathbb{C}$, entonces puesto que $\text{mcd}(2, 12) = 2 \neq 1$, si definiésemos $\chi(a) = 0$ para $\text{mcd}(a, 12) \neq 1$, necesariamente tendríamos $\chi(2) = 0$.

Proposición 6.2.16. Si consideramos al caracter χ como en la Definición 6.2.15, $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ satisface

- (1) $\chi(a) = 0$ si $\text{mcd}(a, f_\chi) \neq 1$.
- (2) $\chi(1) \neq 0$.
- (3) $\chi(ab) = \chi(a)\chi(b)$ para toda $a, b \in \mathbb{Z}$.
- (4) $\chi(a) = \chi(b)$ para $a \equiv b \pmod{f_\chi}$.

Demostración. (1), (2) y (4) son por definición para χ definido módulo f_χ .

Ahora bien, si $a, b \in \mathbb{Z}$, entonces si $\text{mcd}(ab, f_\chi) = 1$, por definición tenemos que $\chi(ab) = \chi(a)\chi(b)$. Si $\text{mcd}(ab, f_\chi) \neq 1$, entonces $\text{mcd}(a, f_\chi) \neq 1$ o $\text{mcd}(b, f_\chi) \neq 1$ y por lo tanto $\chi(a) = 0$ o $\chi(b) = 0$ de donde se sigue $0 = \chi(ab) = \chi(a)\chi(b)$. \square

Observación 6.2.17. Notemos que $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ no es homomorfismo pues $\chi(a+b) \neq \chi(a) + \chi(b)$. Por ejemplo, si χ está definido de la siguiente forma: $\chi: U_3 \rightarrow \mathbb{C}^*$, $\chi(1) = 1$ y $\chi(2) = -1$, entonces $\chi(1+1) = \chi(2) = -1 \neq 2 = 1+1 = \chi(1) + \chi(1)$.

Observación 6.2.18. A menos que se diga lo contrario, el módulo de definición de un caracter de Dirichlet será su conductor, sin embargo cuando hablemos de los caracteres módulo n entenderemos todos los caracteres χ tales que $f_\chi | n$.

También notemos que al definir $\chi(a) = 0$ cuando $\text{mcd}(a, f_\chi) \neq 1$, es definir $\chi(a) = 0$ tan poco como es posible y además $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ es una función periódica de período f_χ : $\chi(a + f_\chi) = \chi(a)$ para toda $a \in \mathbb{Z}$.

Observación 6.2.19. Notemos que si χ no está definido módulo su conductor, entonces χ no tiene período f_χ . Por ejemplo, si consideramos $\chi: U_6 \rightarrow \mathbb{C}^*$ dada por $\chi(1) = 1$ y $\chi(5) = -1$ el cual está definido módulo 6 aunque su conductor f_χ es igual a 3, no tiene período $f_\chi = 3$ pues $1 = \chi(1) \neq \chi(1+3) = \chi(4) = 0$.

Comparar este fenómeno con la Observación 6.2.4.

Definición 6.2.20. El *caracter trivial* es el único caracter de conductor 1, es decir, este es $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ dado por $\chi(a) = 1$ para toda $a \in \mathbb{Z}$.

Definición 6.2.21. Sean χ, ψ dos caracteres con conductores f_χ y f_ψ respectivamente. Sea $\gamma: U_{[f_\chi, f_\psi]} \rightarrow \mathbb{C}^*$ dado por $\gamma(a) := \chi(a)\psi(a)$. Entonces el *producto* $\chi\psi$ es el caracter primitivo asociado a γ . Notemos que γ no tiene por que ser primitivo.

Ejemplo 6.2.22. Sean $\chi: U_8 \rightarrow \mathbb{C}^*$, $U_8 = \{1, 3, 5, 7\}$ dado por $\chi(1) = \chi(3) = 1$; $\chi(5) = \chi(7) = -1$, el cual tiene conductor $f_\chi = 8$ y $\sigma: U_{12} \rightarrow \mathbb{C}^*$, $U_{12} = \{1, 5, 7, 11\}$ dado por $\sigma(1) = \sigma(11) = 1$; $\sigma(5) = \sigma(7) = -1$, el cual tiene conductor $f_\sigma = 12$.

Entonces $[8, 12] = 24$. Definimos $\tilde{\chi}, \tilde{\sigma}$ módulo 24 donde se tiene $U_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Tenemos:

$$\begin{aligned} \pi_{24,8}: U_{24} &\longrightarrow U_8, \\ x \bmod 24 &\longmapsto x \bmod 8, \\ 1, 17 &\longmapsto 1, \\ 5, 13 &\longmapsto 5, \\ 7, 23 &\longmapsto 7, \\ 11, 19 &\longmapsto 3. \end{aligned}$$

Por lo tanto

$$\begin{aligned} \tilde{\chi} &= \chi \circ \pi_{24,8}: U_{24} \longrightarrow \mathbb{C}^*, \\ \tilde{\chi}(1) &= \tilde{\chi}(17) = \chi(1) = 1, \\ \tilde{\chi}(5) &= \tilde{\chi}(13) = \chi(5) = -1, \\ \tilde{\chi}(7) &= \tilde{\chi}(23) = \chi(7) = -1, \\ \tilde{\chi}(11) &= \tilde{\chi}(19) = \chi(3) = 1 \end{aligned}$$

y

$$\begin{aligned} \pi_{24,12}: U_{24} &\longrightarrow U_{12}, \\ x \bmod 24 &\longmapsto x \bmod 12, \\ 1, 13 &\longmapsto 1, \\ 5, 17 &\longmapsto 5, \\ 7, 19 &\longmapsto 7, \\ 11, 23 &\longmapsto 11. \end{aligned}$$

Por lo tanto

$$\begin{aligned} \tilde{\sigma} &= \sigma \circ \pi_{24,12}: U_{24} \longrightarrow \mathbb{C}^*, \\ \tilde{\sigma}(1) &= \tilde{\sigma}(13) = \sigma(1) = 1, \\ \tilde{\sigma}(5) &= \tilde{\sigma}(17) = \sigma(5) = -1, \\ \tilde{\sigma}(7) &= \tilde{\sigma}(19) = \sigma(7) = -1, \\ \tilde{\sigma}(11) &= \tilde{\sigma}(23) = \sigma(11) = 1 \end{aligned}$$

Se sigue que

$$\begin{aligned}
\gamma &= \tilde{\sigma}\tilde{\chi}: U_{24} \longrightarrow \mathbb{C}^*, \\
\gamma(1) &= \tilde{\sigma}(1)\tilde{\chi}(1) = 1, \\
\gamma(5) &= \tilde{\sigma}(5)\tilde{\chi}(5) = 1, \\
\gamma(7) &= \tilde{\sigma}(7)\tilde{\chi}(7) = 1, \\
\gamma(11) &= \tilde{\sigma}(11)\tilde{\chi}(11) = 1, \\
\gamma(13) &= \tilde{\sigma}(13)\tilde{\chi}(13) = -1, \\
\gamma(17) &= \tilde{\sigma}(17)\tilde{\chi}(17) = -1, \\
\gamma(19) &= \tilde{\sigma}(19)\tilde{\chi}(19) = -1, \\
\gamma(23) &= \tilde{\sigma}(23)\tilde{\chi}(23) = -1.
\end{aligned}$$

En este caso γ es primitivo, $f_\gamma = 24$, y γ es el producto de χ y σ : $\gamma = \chi\sigma$.

Ejemplo 6.2.23. Sean ahora $\theta: U_3 \rightarrow \mathbb{C}^*$ dada por $\theta(1) = 1$, $\theta(2) = -1$ y $\sigma: U_{12} \rightarrow \mathbb{C}^*$ como en el Ejemplo 6.2.22. Entonces $f_\theta = 3$, $f_\sigma = 12$ y $[3, 12] = 12$. Sea $\tilde{\theta} = \theta \circ \pi_{12,3}$ y $\tilde{\sigma} = \sigma$. Entonces $\gamma = \tilde{\sigma}\tilde{\theta}: U_{12} \rightarrow \mathbb{C}^*$ está dada por

$$\begin{aligned}
\tilde{\sigma}\tilde{\theta}(1) &= \tilde{\sigma}(1)\tilde{\theta}(1) = 1, \\
\tilde{\sigma}\tilde{\theta}(5) &= \tilde{\sigma}(5)\tilde{\theta}(5) = 1, \\
\tilde{\sigma}\tilde{\theta}(7) &= \tilde{\sigma}(7)\tilde{\theta}(7) = -1, \\
\tilde{\sigma}\tilde{\theta}(11) &= \tilde{\sigma}(11)\tilde{\theta}(11) = -1.
\end{aligned}$$

Ahora bien γ puede ser definido módulo 4: Sea $\xi: U_4 \rightarrow \mathbb{C}^*$, dada por $\xi(1) = 1$, $\xi(3) = -1$. Entonces $\xi \circ \pi_{12,4} = \gamma$. Por lo tanto γ no es primitivo. Se sigue que $\xi = \theta\sigma$ y $f_\xi = 4$.

Definición 6.2.24. Sea $\chi: U_n \rightarrow \mathbb{C}^*$ cualquier caracter de Dirichlet definido módulo n . Definimos el *conjugado* de χ por

$$\bar{\chi}: U_n \longrightarrow \mathbb{C}^*, \quad \bar{\chi}(a) := \overline{\chi(a)} = \chi(a)^{-1}.$$

Entonces $\chi\bar{\chi}$ es el caracter trivial y $f_{\chi\bar{\chi}} = 1$.

El siguiente resultado es muy útil para el cálculo de conductores.

Teorema 6.2.25. Sean χ, ψ dos caracteres de Dirichlet cuyos conductores son primos relativos $\text{mcd}(f_\chi, f_\psi) = 1$. Entonces $f_{\chi\psi} = f_\chi f_\psi$.

Demostración. Sean $n = f_\chi$, $m = f_\psi$. Entonces $\chi: U_n \rightarrow \mathbb{C}^*$, $\psi: U_m \rightarrow \mathbb{C}^*$. Se define $\gamma: U_{[n,m]} = U_{nm} \rightarrow \mathbb{C}^*$ por $\gamma(a) := \tilde{\chi}(a)\tilde{\psi}(a)$ donde $\tilde{\chi} = \chi \circ \pi_{nm,n}$, $\tilde{\psi} = \psi \circ \pi_{nm,m}$. Definimos $\varphi = \gamma\chi^{-1}: U_{[n,m],n} = U_{[nm,n]} = U_{nm} \rightarrow \mathbb{C}^*$. Se tiene que

$$\begin{aligned}\varphi(a \bmod nm) &= \gamma(a \bmod nm) \tilde{\chi}^{-1}(a \bmod nm) = \\ &= \tilde{\chi}(a \bmod nm) \tilde{\psi}(a \bmod nm) \tilde{\chi}^{-1}(a \bmod nm) = \tilde{\psi}(a \bmod nm).\end{aligned}$$

Es decir, $\varphi = \tilde{\psi}$. Por tanto $f_\varphi = f_{\tilde{\psi}} = f_\psi = m$.

Ahora bien, $f_{\chi\psi} | [f_\chi, f_\psi] = nm$, por lo tanto

$$m = f_\psi = f_\varphi = f_{(\chi\psi)\chi^{-1}} | [f_{\chi\psi}, f_{\chi^{-1}}] = [f_{\chi\psi}, f_\chi] = [f_{\chi\psi}, n] = \frac{f_{\chi\psi} n}{\text{mcd}(f_{\chi\psi}, n)}.$$

Sea $r := \frac{f_{\chi\psi} n}{\text{mcd}(f_{\chi\psi}, n)}$. Entonces $m | rn$ y $\text{mcd}(m, n) = 1$ por lo que $m | r$. También tenemos que

$$m | \frac{f_{\chi\psi} n}{\text{mcd}(f_{\chi\psi}, n)} = f_{\chi\psi} \frac{n}{\text{mcd}(f_{\chi\psi}, n)} = f_{\chi\psi} n_1 \quad \text{con} \quad n_1 | n.$$

Nuevamente, del hecho de que $\text{mcd}(m, n) = 1$, se sigue que $m | f_{\chi\psi}$.

Similarmente, se tiene que $n | f_{\chi\psi}$ y puesto que $\text{mcd}(m, n) = 1$, $mn = [f_\chi, f_\psi] | f_{\chi\psi}$. Se sigue que $f_{\chi\psi} = nm = f_\chi f_\psi$. \square

Definición 6.2.26. Un caracter $\chi: G \rightarrow \mathbb{C}^*$ se dice que es un *caracter de Galois* si G es el grupo de Galois de una extensión finita de campos L/K : $G = \text{Gal}(L/K)$.

Tenemos que los caracteres de Dirichlet pueden ser vistos como caracteres de Galois pues si χ es un caracter de Dirichlet, $\chi: U_n \rightarrow \mathbb{C}^*$, entonces $U_n \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Veamos como podemos usar los caracteres de Dirichlet para estudiar la aritmética de la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Ejemplo 6.2.27. Se tiene que $U_8 \cong \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$. Sea $\chi: U_8 \rightarrow \mathbb{C}^*$ el caracter dado por $\chi(1) = \chi(7) = 1$ y $\chi(3) = \chi(5) = -1$.

Se tiene que $\text{nuc } \chi = \{1, 7 \bmod 8\}$. Notemos que

$$\text{nuc } \chi \cong \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2})) = \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_8)^+) \cong \{\pm 1 \bmod 8\}.$$

Por tanto χ es un caracter de $\frac{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}))} \cong \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Más precisamente, si $G = \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$, $\chi: G \rightarrow \mathbb{C}^*$ y $H = \text{nuc } \chi < G$, χ se factoriza:

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \nearrow \tilde{\chi} \\ & G/H & \end{array} \quad \tilde{\chi}: G/H \rightarrow \mathbb{C}^*, \quad \tilde{\chi} \circ \pi = \chi$$

y $G/H \cong \text{Gal}(\mathbb{Q}(\zeta_8)^H/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Similarmente, si $\varphi: U_8 \rightarrow \mathbb{C}^*$ está dado por $\varphi(1) = \varphi(5) = 1$ y $\varphi(3) = \varphi(7) = -1$, entonces $\text{núc } \varphi = \{1, 5 \bmod 8 \mid 8\}$ y $\text{núc } \varphi \cong \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)) = \{x \bmod 8 \mid x \equiv 1 \bmod 4\} = D_{8,4}$ y por tanto φ es un caracter de

$$\frac{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))} \cong \text{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \cong U_4.$$

Notemos que $f_\varphi = 4$ y que $f_\chi = 8$.

Sea χ un caracter de Dirichlet definido módulo n , $\chi: U_n \rightarrow \mathbb{C}^*$. Entonces, si $H = \text{núc } \chi$, χ es un caracter de Galois de $\text{Gal}(\mathbb{Q}(\zeta_n)^H/\mathbb{Q})$:

$$\begin{array}{ccc} U_n \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \nearrow \tilde{\chi} \\ & U_n / \text{núc } \chi & \end{array}$$

$$U_n/H \cong U_n/(\text{núc } \chi) = \frac{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^H)} \cong \text{Gal}(\mathbb{Q}(\zeta_n)^H/\mathbb{Q}).$$

Definición 6.2.28. Sea $\chi: U_n \rightarrow \mathbb{C}^*$ un caracter de Dirichlet. Se define el campo que pertenece a χ o que está asociado a χ por $K := \mathbb{Q}(\zeta_n)^{\text{núc } \chi} \subseteq \mathbb{Q}(\zeta_n)$.

Teorema 6.2.29. Sea $\chi: U_n \rightarrow \mathbb{C}^*$ un caracter de Dirichlet con conductor $f := f_\chi \mid n$. Sea $\tilde{\chi}$ el caracter primitivo asociado a χ : $\tilde{\chi} \circ \pi_{n,f} = \chi$. Entonces los campos asociados a $\tilde{\chi}$ y a χ son el mismo. En particular, el campo asociado a χ depende únicamente de χ y no de módulo en donde está definido.

Demostración. El resultado se sigue inmediatamente de la Observación 6.2.30. Presentamos aquí la prueba por completos.

Puesto que $\tilde{\chi} \circ \pi_{n,f} = \chi$, se tiene que $\text{núc } \chi = \pi_{n,f}^{-1}(\text{núc } \tilde{\chi})$. Sean K y L los campos asociados a χ y $\tilde{\chi}$ respectivamente: $K := \mathbb{Q}(\zeta_n)^{\text{núc } \chi}$, $L := \mathbb{Q}(\zeta_n)^{\text{núc } \tilde{\chi}}$. Primero notemos que

$$\begin{aligned} [K : \mathbb{Q}] &= \left| \frac{U_n}{\text{núc } \chi} \right| = \frac{|U_n|}{|\pi_{n,f}^{-1}(\text{núc } \tilde{\chi})|} = \frac{|U_n|}{|\text{núc } \pi_{n,f}| |\text{núc } \tilde{\chi}|} \\ &= \frac{|U_f|}{|\text{núc } \tilde{\chi}|} = [L : \mathbb{Q}]. \end{aligned}$$

Por otro lado, si $\alpha \in L$, $\sigma\alpha = \alpha$ para toda $\sigma \in \text{núc } \tilde{\chi}$. Sea $\theta \in \text{núc } \chi$. Entonces $\pi_{n,f}\theta \in \text{núc } \tilde{\chi}$, por lo tanto $(\pi_{n,f}\theta)(\alpha) = \alpha = \pi_{n,f}(\theta(\alpha)) = \tilde{\theta}(\alpha)$. Por lo tanto $L \subseteq K$ de donde se sigue que $L = K$.

La última parte se sigue inmediatamente pues todos los caracteres de Dirichlet están unívocamente determinados por el caracter primitivo asociado. \square

Observación 6.2.30. De hecho lo establecido en el Teorema 6.2.29 sucede en general. Si $G := \text{Gal}(F/E)$, y $\pi: G \rightarrow G_1$ es un epimorfismo, $G_1 \cong G/H$. Si $M = F^H$, se tiene para $R \subseteq G/H$ que $M^R = F^{\pi^{-1}(R)}$.

$$\begin{array}{c} F \\ \downarrow H \\ M \\ \downarrow \\ E \end{array}$$

Observación 6.2.31. Notemos que si χ es un caracter de Dirichlet y $X := \langle \chi \rangle$ es el grupo generado por χ , entonces $\bigcap_{\varphi \in X} \text{núc } \varphi = \bigcap_{i=0}^{t-1} \text{núc } \chi^i$ donde $o(\chi) = t$. Se tiene que $\text{núc } \chi^i \supseteq \text{núc } \chi$ por lo que $\bigcap_{\varphi \in X} \text{núc } \varphi = \text{núc } \chi$. En otras palabras $\mathbb{Q}(\zeta_n)^{\bigcap_{\varphi \in X} \text{núc } \varphi} = \mathbb{Q}(\zeta_n)^{\text{núc } \chi}$.

Más generalmente, si Y es cualquier conjunto de caracteres de Dirichlet y si $X := \langle Y \rangle$ es el grupo generado por los elementos de Y , entonces si $n := \text{mcm}[\text{f}_\chi \mid \chi \in Y]$ y todos los elementos de Y los consideramos módulo n , se sigue que X es un grupo de caracteres módulo n , es decir, $X \subseteq \hat{U}_n$. En este caso, con el argumento anterior, se tiene que $\mathbb{Q}(\zeta_n)^{\bigcap_{\chi \in Y} \text{núc } \chi} = \mathbb{Q}(\zeta_n)^{\bigcap_{\chi \in X} \text{núc } \chi}$.

Definición 6.2.32. Sea X cualquier grupo de caracteres de Dirichlet definidos módulo n . Entonces se define el *campo que pertenece a X* o el *campo asociado a X* por $K := \mathbb{Q}(\zeta_n)^H$ donde $H = \bigcap_{\chi \in X} \text{núc } \chi$.

Como antes, si Y es un conjunto arbitrario de caracteres de Dirichlet, entonces $H = \bigcap_{\chi \in Y} \text{núc } \chi = \bigcap_{\chi \in \langle Y \rangle = X} \text{núc } \chi$.

Como veremos a continuación, si X es un grupo de caracteres de Dirichlet y K es su campo asociado, entonces

$$X = \widehat{\text{Gal}(K/\mathbb{Q})} \cong \text{Gal}(K/\mathbb{Q})$$

y en particular $|X| = [K : \mathbb{Q}]$.

Ejemplo 6.2.33. Sea χ un caracter de orden 2 y definido módulo n : $\chi \in \hat{U}_n$, $\chi^2 = 1$, $\chi \neq 1$. Entonces $\chi(U_n) = \{\pm 1\}$ y $\text{núc } \chi = H = \{a \in U_n \mid \chi(a) = 1\}$. Se tiene que $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^H) \cong H$ y por tanto $\text{Gal}(\mathbb{Q}(\zeta_n)^H/\mathbb{Q}) \cong \frac{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^H)} \cong U_n/H \cong \langle \tilde{\chi} \rangle$ donde $\tilde{\chi}$ es la factorización de χ :

$$\begin{array}{ccc} U_n & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \pi & \nearrow \tilde{\chi} \\ & U_n/H \cong U_n/(\text{núc } \chi) & \end{array}$$

Por tanto K , el campo cuadrático que pertenece a χ , es una extensión cuadrática de \mathbb{Q} contenida en $\mathbb{Q}(\zeta_n)$. En particular, si n es un primo impar, $n = p$, entonces $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ (ver Sección 5.3.3).

Ejemplo 6.2.34. Consideremos $\mathbb{Q}(\zeta_n)^+$ el subcampo real de $\mathbb{Q}(\zeta_n)$. Entonces $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n)^{\{1, J\}}$ donde J denota conjugación compleja. Entonces $\mathbb{Q}(\zeta_n)^+$ pertenece al conjunto de caracteres $X \subseteq \hat{U}_n \cong \text{Gal}(\widehat{\mathbb{Q}(\zeta_n)}/\mathbb{Q})$ tales que $\bigcap_{\chi \in X} \text{núc } \chi = \{1, J\} = \{\pm 1\}$, esto es a $X = \{\chi \mid \chi(-1) = 1\}$. En otras palabras, bajo el mapeo

$$\begin{aligned} U_n \times \hat{U}_n &\longrightarrow \mathbb{C}^* \\ (a, \sigma) &\longmapsto \sigma(a) \end{aligned}$$

se tiene $X = \{\pm 1\}^\perp$ (ver Definición 6.1.10).

Ahora bien, si χ es cualquier caracter definido módulo n , y si K es el campo asociado a χ , se tiene que

$$K \subseteq \mathbb{R} \iff \text{el mapeo } \zeta_n \xrightarrow{\sigma} \zeta_n^{-1}, \text{ satisface } \sigma \in \text{núc } \chi \iff \chi(-1) = 1.$$

Es decir, K es real si y solamente si χ es par.

Ejemplo 6.2.35. Consideremos en $\mathbb{Q}(\zeta_8)$ el subcampo cuadrático real, esto es, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8)^+$. Entonces $\mathbb{Q}(\sqrt{2})$ es el campo que pertenece al caracter dado por $\chi: U_8 \rightarrow \mathbb{C}^*$, $\chi(1) = \chi(7) = 1$ y $\chi(3) = \chi(5) = -1$ pues $7 \equiv -1 \pmod{8}$ y $\chi(-1) = 1$ y $\mathbb{Q}(\sqrt{2})$ es un campo real.

Notemos que $f_\chi = 8$ pues el único caracter de conductor 4 necesariamente tiene como su campo asociado a $\mathbb{Q}(\zeta_4)$.

Ejemplo 6.2.36. En $\mathbb{Q}(\zeta_{12})$, tenemos que $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3, \zeta_4) = \mathbb{Q}(\sqrt{3}, \sqrt{-3})$. Hay tres subcampos cuadráticos de $\mathbb{Q}(\zeta_{12})$, a saber: $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ y $\mathbb{Q}(\zeta_{12})^+ = \mathbb{Q}(\sqrt{3})$.

Entonces al considerar el caracter $\chi: U_{12} \rightarrow \mathbb{C}^*$, $\chi(1) = \chi(11) = 1$ y $\chi(5) = \chi(7) = -1$, tenemos que $\text{núc } \chi = \{1, 11\}$ y $o(\chi) = 2$. Puesto que $\chi(11) = \chi(-1) = 1$ el campo que pertenece a χ es $K = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\zeta_{12})^+ = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$.

Otra forma de concluir lo mismo, es notar que hay tres caracteres cuadráticos módulo 12, pero dos de ellos tienen conductores 3 (el asociado a $\mathbb{Q}(\zeta_3)$) y 4 (el asociado a $\mathbb{Q}(\zeta_4)$). Puesto que el conductor de χ es 12 se concluye que el campo asociado es necesariamente $\mathbb{Q}(\sqrt{3})$.

Nuestro siguiente objetivo es mostrar que si X es un grupo de caracteres entonces $X \cong \text{Gal}(\widehat{K}/\mathbb{Q})$ donde K es el campo asociado a X . Para ello consideraremos un mapeo bilineal no degenerado.

Sea pues X un grupo de caracteres de Dirichlet y sea K el campo asociado a X , es decir, $K = \mathbb{Q}(\zeta_n)^H$ donde $n = \text{mcm}\{f_\chi \mid \chi \in X\}$, $H = \bigcap_{\chi \in X} \text{núc } \chi$.

Sea $\varphi: \text{Gal}(K/\mathbb{Q}) \times X \longrightarrow \mathbb{C}^*$
 $(\sigma, \chi) \longmapsto \chi(\sigma)$ el mapeo natural. Veamos que φ está bien definido.

Se tiene que $\sigma \in \text{Gal}(K/\mathbb{Q}) \cong U_n/H$. Ahora bien $\chi \in X \subseteq \hat{U}_n$, es decir, $\chi: U_n \rightarrow \mathbb{C}^*$. Puesto que $H \subseteq \text{núc } \chi$, es decir, $\chi(H) = 1$, se tiene que χ se factoriza de manera única: $\tilde{\chi} \circ \pi = \chi$.

$$\begin{array}{ccc}
 U_n & \xrightarrow{\chi} & \mathbb{C}^* \\
 & \searrow \pi & \nearrow \tilde{\chi} \\
 & U_n/H &
 \end{array}
 \quad
 \begin{array}{c}
 \left\{ \begin{array}{c}
 \mathbb{Q}(\zeta_n) \\
 \downarrow H \\
 K \\
 \downarrow \left. \vphantom{\begin{array}{c} K \\ \downarrow \end{array}} \right\} U_n/H \\
 \mathbb{Q}
 \end{array} \right.
 \end{array}$$

y por tanto $\chi(\sigma)$ está bien definido.

Teorema 6.2.37. *Se tiene que φ es un mapeo bilineal no degenerado, esto es, si $\chi(\sigma) = 1$ para toda $\sigma \in G := \text{Gal}(K/\mathbb{Q})$, entonces $\chi = 1$ y si $\chi(\sigma) = 1$ para toda $\chi \in X$, entonces $\sigma = \text{Id}_K$.*

Demostración. Es inmediato que φ es bilineal. Ahora bien, si $\chi(\sigma) = 1$ para toda $\sigma \in G \cong U_n/H$, entonces $\chi: U_n \rightarrow \mathbb{C}^*$ es trivial pues $\chi(H) = 1$ y al factorizar χ a través de H , $\tilde{\chi}: U_n/H \rightarrow \mathbb{C}^*$, $\tilde{\chi}(\sigma) = 1$ para toda $\sigma \in U_n/H$, por lo que $\chi = 1$.

Recíprocamente, si $\chi(\sigma) = 1$ para toda $\chi \in X$, entonces se tiene que $\sigma \in \bigcap_{\chi \in X} \text{núcl } \chi = H$, por lo tanto $\bar{\sigma} = 1$ en $U_n/H = G$. \square

Corolario 6.2.38. *Se tiene que $X \cong \hat{G} = \widehat{\text{Gal}(K/\mathbb{Q})}$ y en particular $|X| = [K : \mathbb{Q}]$.*

Demostración. Esto no es más que una aplicación del Teorema 6.1.9. \square

El mismo mapeo φ nos sirve, como vimos en general, para dar un isomorfismo de redes entre los subcampos de K y los subgrupos de X . Más precisamente, sea $F \subseteq K$.

$$\begin{array}{c}
 K \\
 \downarrow \\
 F \\
 \downarrow \\
 \mathbb{Q}
 \end{array}$$

Sea $Y = \{\chi \in X \mid \chi(g) = 1 \ \forall g \in \text{Gal}(K/F)\}$. Entonces, $Y =$

$\text{Gal}(K/F)^\perp \cong \left(G / \widehat{\text{Gal}(K/F)} \right) \cong \widehat{\text{Gal}(F/\mathbb{Q})}$ (Definición 6.1.10, Proposición 6.1.11).

Recíprocamente, dado Y un subgrupo de X , sea F el campo fijo bajo el ortogonal de Y : $F := K^{Y^\perp}$, donde recordemos que $Y^\perp = \{g \in G \mid \chi(g) = 1 \ \forall \chi \in Y\}$. Por tanto $\text{Gal}(K/F) = \text{Gal}(K/K^{Y^\perp}) \cong Y^\perp$. Por la Proposición 6.1.13 tenemos

$$Y = Y^{\perp\perp} = \text{Gal}(K/F)^\perp = \widehat{\text{Gal}(F/\mathbb{Q})}.$$

Esta correspondencia es biyectiva como lo prueba el siguiente resultado.

Teorema 6.2.39. *Existe una biyección entre los subgrupos de X y los subcampos de K dada por*

$$\begin{aligned}\mathrm{Gal}(K/F)^\perp &\longleftarrow L \\ Y &\longrightarrow K^{Y^\perp}\end{aligned}$$

Demostración. Sean $\mathcal{A} = \{Y \mid Y < X\}$ y $\mathcal{B} = \{F \mid F \text{ es subcampo de } K\}$. Sean

$$\begin{array}{ccc}\mathcal{A} & \xrightarrow{\theta} & \mathcal{B} \\ Y & \longmapsto & K^{Y^\perp}\end{array} \qquad \begin{array}{ccc}\mathcal{B} & \xrightarrow{\delta} & \mathcal{A} \\ F & \longmapsto & \mathrm{Gal}(K/F)^\perp\end{array}$$

Se tiene que

$$(\theta \circ \delta)(F) = \theta(\mathrm{Gal}(K/F)^\perp) = K^{(\mathrm{Gal}(K/F)^\perp)^\perp} = K^{\mathrm{Gal}(K/F)} = F$$

y

$$(\delta \circ \theta)(Y) = \delta(K^{Y^\perp}) = \mathrm{Gal}(K/K^\perp)^\perp = (Y^\perp)^\perp = Y$$

lo cual demuestra que θ y δ son biyecciones, cada una de ellas inversa de la otra. \square

Observación 6.2.40. Se tiene que el isomorfismo

$$Y = \widehat{\mathrm{Gal}(F/\mathbb{Q})} \cong \mathrm{Gal}(F/\mathbb{Q})$$

para $Y < X$, se expresa a través del mapeo bilineal

$$\begin{aligned}\mu: \mathrm{Gal}(F/\mathbb{Q}) \times Y &\longrightarrow \mathbb{C}^* \\ (g, \sigma) &\longmapsto \mu(g, \sigma) := \sigma(g).\end{aligned}$$

Proposición 6.2.41. *Sean X_1, X_2 dos grupos de caracteres de Dirichlet y sean K_1, K_2 sus campos asociados. Entonces*

- (1) $X_1 \subseteq X_2 \iff K_1 \subseteq K_2$,
- (2) $X_1 \cap X_2$ corresponde al campo $K_1 \cap K_2$,
- (3) El grupo generado por X_1 y X_2 : $\langle X_1, X_2 \rangle = X_1 \cdot X_2$, corresponde al campo generado por K_1 y K_2 : $K_1 K_2$.

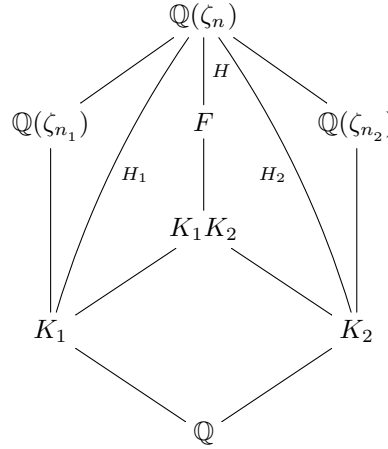
Demostración. Sea $X := \langle X_1, X_2 \rangle$ y F es campo correspondiente a X . Más precisamente, sean

$$n := \mathrm{mcm}\{\mathfrak{f}_\chi \mid \chi \in X\}, \quad n_i := \mathrm{mcm}\{\mathfrak{f}_\chi \mid \chi \in X_i\}, \quad i = 1, 2.$$

Entonces $n_i \mid n$, $i = 1, 2$. Sean

$$H_1 = \bigcap_{\chi \in X_1} \text{núc } \chi, \quad H_2 = \bigcap_{\chi \in X_2} \text{núc } \chi, \quad H = \bigcap_{\chi \in X} \text{núc } \chi,$$

$$K_1 = \mathbb{Q}(\zeta_n)^{H_1}, \quad K_2 = \mathbb{Q}(\zeta_n)^{H_2}.$$



Se tiene que si $X_1 \subseteq X_2$ entonces $H_1 \supseteq H_2$ y por tanto $\mathbb{Q}(\zeta_n)^{H_1} \subseteq \mathbb{Q}(\zeta_n)^{H_2}$ lo cual nos dice que $K_1 \subseteq K_2$.

Recíprocamente, si $K_1 \subseteq K_2$, entonces $K_1 = \mathbb{Q}(\zeta_n)^{H_1} \subseteq \mathbb{Q}(\zeta_n)^{H_2} = K_2$ y por tanto $H_1 = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^{H_1}) \supseteq \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^{H_2}) = H_2$. Ahora queremos ver que $H_1 \supseteq H_2$ si y solamente si $X_1 \subseteq X_2$ lo cual implicará (1).

Del mapeo bilineal $\varphi: \text{Gal}(F/\mathbb{Q}) \times X \rightarrow \mathbb{C}^*$, $\varphi(\sigma, \chi) = \chi(\sigma)$ obtenemos

$$\begin{aligned} X_i^\perp &= \{g \in \text{Gal}(F/\mathbb{Q}) \mid \chi(g) = 1 \ \forall \ \chi \in X_i\} \\ &= \{g \in \text{Gal}(F/\mathbb{Q}) \mid g \in \text{núc } \chi \ \forall \ \chi \in X_i\} \\ &= \bigcap_{\chi \in X_i} \text{núc } \chi = H_i, \quad i = 1, 2, \end{aligned}$$

es decir, $H_i = X_i^\perp$. Se sigue que si $H_1 \supseteq H_2$, entonces $X_1^\perp \supseteq X_2^\perp$ lo cual implica que $(X_1^\perp)^\perp = X_1 \subseteq X_2 = (X_2^\perp)^\perp$ que a su vez demuestra que $K_1 \subseteq K_2$ implica $X_1 \subseteq X_2$.

Con esto terminamos la demostración de (1).

Para ver (2), sea F el campo asociado a $X_1 \cap X_2$. Puesto que $X_1 \cap X_2 \subseteq X_i$, $i = 1, 2$, se sigue de (1) que $F \subseteq K_1 \cap K_2$. Ahora bien, si W es el grupo de caracteres de Dirichlet asociado a $K_1 \cap K_2$, por (1) nuevamente, se tiene $W \subseteq X_i$, $i = 1, 2$ de donde obtenemos que $W \subseteq X_1 \cap X_2$ y por (1) se sigue que $K_1 \cap K_2 \subseteq F$. Esto es (2).

Para probar (3), sabemos por Teoría de Galois que se tiene $K_1 K_2 = \mathbb{Q}(\zeta_n)^{H_1} \mathbb{Q}(\zeta_n)^{H_2} = \mathbb{Q}(\zeta_n)^{H_1 \cap H_2}$ y $H_1 \cap H_2 = X_1^\perp \cap X_2^\perp$. Veamos que $(X_1 \cup X_2)^\perp = \langle X_1, X_2 \rangle^\perp$. Notemos que $(X_1 \cup X_2)^\perp = \{\sigma \in G \mid \chi(\sigma) = 1 \text{ para toda } \sigma \in X_1 \cap X_2\}$, por lo que $\chi(\sigma) = 1$ para toda $\sigma \in \langle X_1, X_2 \rangle$ lo cual prueba que $(X_1 \cup X_2)^\perp \subseteq \langle X_1, X_2 \rangle^\perp$.

Ahora si $\sigma \in \langle X_1, X_2 \rangle^\perp$ entonces $\chi(\sigma) = 1$ para todo $\sigma \in \langle X_1, X_2 \rangle$ y por tanto $\chi(\sigma) = 1$ para todo $\chi \in X_1 \cup X_2$. Se sigue que $\langle X_1, X_2 \rangle^\perp \subseteq (X_1 \cup X_2)^\perp$ y obtenemos la igualdad.

Por otro lado, puesto que $X_i \subseteq X_1 \cup X_2$ si sigue que $X_i^\perp \supseteq (X_1 \cup X_2)^\perp$. Se sigue que $X_1^\perp \cap X_2^\perp \supseteq (X_1 \cup X_2)^\perp$. Recíprocamente, si $\sigma \in X_1^\perp \cap X_2^\perp$ entonces $\chi_1(\sigma) = 1$ y $\chi_2(\sigma) = 1$ para cualesquiera $\chi_i \in X_i$, $i = 1, 2$. De esta manera obtenemos que $\chi(\sigma) = 1$ para todo $\chi \in X_1 \cup X_2$ y en particular $\sigma \in (X_1 \cup X_2)^\perp$. Esto prueba que $X_1^\perp \cap X_2^\perp = (X_1 \cup X_2)^\perp$.

Por lo anterior, tenemos que $H_1 \cap H_2 = X_1^\perp \cap X_2^\perp = (X_1 \cup X_2)^\perp = \langle X_1, X_2 \rangle^\perp = X^\perp$ y se sigue que $K_1 K_2$ corresponde a $X = \langle X_1, X_2 \rangle$. \square

Proposición 6.2.42. *Sea K/\mathbb{Q} una extensión abeliana y sea X el grupo de caracteres de Dirichlet asociado a K . Sea $n = \text{mcd}\{\mathfrak{f}_\chi \mid \chi \in X\}$. Entonces n es el mínimo natural tal que $K \subseteq \mathbb{Q}(\zeta_n)$.*

Demostración. Si $K \subseteq \mathbb{Q}(\zeta_m)$ entonces todo caracter $\chi \in X$ pueda ser definido módulo m y por tanto $\mathfrak{f}_\chi \mid m$. Se sigue que $n \mid m$. \square

6.3. Aritmética de $\mathbb{Q}(\zeta_n)$ usando caracteres

Los caracteres de Dirichlet resultan ser una herramienta poderosa para el estudio de las extensiones abelianas de \mathbb{Q} .

Sea $n \in \mathbb{N}$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su descomposición en primos. Entonces $U_n \xrightarrow{\phi} U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}$. Sea $\chi \in \hat{U}_n$, $\chi: U_n \rightarrow \mathbb{C}^*$. Sea $g_{p_i}: U_{p_i^{\alpha_i}} \rightarrow U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}$ dado por $g_{p_i}(x) = (1, \dots, 1, \overset{i}{x}, 1, \dots, 1)$.

El isomorfismo $\phi: U_n \rightarrow U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}}$ está dado por el Teorema Chino del Residuo: $\phi(x \bmod n) = (x \bmod p_1^{\alpha_1}, \dots, x \bmod p_r^{\alpha_r})$. Se tiene el diagrama conmutativo

$$\begin{array}{ccccc} U_n & \xrightarrow{\phi} & U_{p_1^{\alpha_1}} \times \cdots \times U_{p_r^{\alpha_r}} & \xleftarrow{g_{p_i}} & U_{p_i^{\alpha_i}} \\ & \searrow \chi & & \swarrow \chi_{p_i} & \\ & & \mathbb{C}^* & & \end{array}$$

donde $\chi_{p_i}: U_{p_i^{\alpha_i}} \rightarrow \mathbb{C}^*$ está dado por:

$$\chi_{p_i} := \chi \circ \phi^{-1} \circ g_{p_i}.$$

Si $a \in \mathbb{Z}$ es primo relativo a n , entonces

$$\chi_{p_i}(a) = \chi(\phi(g_{p_i}(a \bmod p_i^{\alpha_i}))) = \chi(\phi^{-1}(1, \dots, 1, a, 1, \dots, 1)) = \chi(b_i)$$

donde $b_i \in \mathbb{Z}$ satisface:

$$\begin{aligned} b_i &\equiv 1 \pmod{p_j^{\alpha_j}}, \quad j = 1, \dots, r, \quad j \neq i, \\ b_i &\equiv a_i \pmod{p_i^{\alpha_i}}. \end{aligned}$$

Notemos que $b_1 \cdots b_i \cdots b_r \equiv 1 \cdots a \cdots 1 \equiv a \pmod{p_i^{\alpha_i}}$ para toda $1 \leq i \leq r$, lo cual implica que $b_1 \cdots b_r \equiv a \pmod{n}$. Por lo tanto

$$\chi(a) = \chi(b_1 \cdots b_r) = \chi(b_1) \cdots \chi(b_r) = \chi_{p_1}(a) \cdots \chi_{p_r}(a) = (\chi_{p_1} \cdots \chi_{p_r})(a).$$

Se sigue que $\chi = \chi_{p_1} \chi_{p_2} \cdots \chi_{p_r}$.

Por el Teorema 6.2.25 se tiene que $f_\chi = \prod_{i=1}^r f_{\chi_{p_i}}$. En particular $p \mid f_\chi$ si y solamente si χ_{p_i} es no trivial.

Definición 6.3.1. Con la notación anterior, si X es un grupo de caracteres módulo n y si p es un número primo, entonces se define

$$X_p := \{\chi_p \mid \chi \in X\}.$$

Notemos que $X_p = \{1\}$ si $p \notin \{p_1, \dots, p_r\}$.

Ejemplo 6.3.2. Sea $\chi: U_{12} \rightarrow \mathbb{C}^*$ el caracter cuadrático par, es decir $\chi(1) = \chi(11) = 1$, $\chi(5) = \chi(7) = -1$.

Se tiene que $12 = 2^2 \cdot 3$. Entonces $\chi = \chi_2 \chi_3$, donde $\chi_2: U_4 \rightarrow \mathbb{C}^*$, $\chi_3: U_3 \rightarrow \mathbb{C}^*$. Calculemos χ_2 y χ_3 . Se tiene

$$\begin{array}{ccccc} U_4 & \xrightarrow{g_2} & U_4 \times U_3 & \xrightarrow{\phi^{-1}} & U_{12} \\ 1 & \mapsto & (1, 1) & \mapsto & 1 \\ 3 & \mapsto & (3, 1) & \mapsto & 7 \end{array}$$

pues $7 \equiv 3 \pmod{4}$, $7 \equiv 1 \pmod{3}$,

$$\begin{array}{ccccc} U_3 & \xrightarrow{g_3} & U_4 \times U_3 & \xrightarrow{\phi^{-1}} & U_{12} \\ 1 & \mapsto & (1, 1) & \mapsto & 1 \\ 2 & \mapsto & (1, 2) & \mapsto & 5 \end{array}$$

pues $5 \equiv 1 \pmod{4}$, $5 \equiv 2 \pmod{3}$.

Por tanto

$$\begin{aligned} \chi_2 &= \chi \circ \phi^{-1} \circ g_2, \quad \chi_2(1) = 1, \quad \chi_2(3) = \chi(7) = -1, \\ \chi_3 &= \chi \circ \phi^{-1} \circ g_3, \quad \chi_3(1) = 1, \quad \chi_3(3) = \chi(5) = -1. \end{aligned}$$

Entonces $X := \langle \chi \rangle$, $X_2 := \langle \chi_2 \rangle$, $X_3 := \langle \chi_3 \rangle$ y si p es cualquier primo, $p \neq 2, 3$, $X_p = \{1\}$.

El resultado más importante, es la relación entre X_p y el índice de ramificación de p en K/\mathbb{Q} , donde K es el campo asociado a X .

Teorema 6.3.3. Sea X un grupo de caracteres de Dirichlet y sea K el campo asociado a X . Sea p un número primo y sea e el índice de ramificación de p en K/\mathbb{Q} . Entonces $e = |X_p|$.

Demostración. Sea $n := \text{mcm}\{f_\chi \mid \chi \in X\}$. Entonces $K \subseteq \mathbb{Q}(\zeta_n)$. Escribamos $n = p^a m$ con $\text{mcd}(m, p) = 1$. Definimos $L := K(\zeta_m) = K\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Si Y es el grupo de caracteres módulo n asociado al campo L , entonces por el Teorema 6.2.39 se tiene que $L = \mathbb{Q}(\zeta_n)^{Y^\perp}$.

Ahora bien, puesto que $L = K\mathbb{Q}(\zeta_m)$, por la Proposición 6.2.41 se tiene que el grupo de caracteres Y está generado por X y por los caracteres de $\mathbb{Q}(\zeta_n)$ de conductor un divisor de m , los cuales son precisamente \hat{U}_m .

Si $\varphi \in Y$, entonces $\varphi = \chi\psi$ con $\chi \in X$ y $\psi \in \hat{U}_m$. Escribamos $\chi = \chi_p\chi'$ con $\chi' = \prod_{q|m} \chi_q \in \hat{U}_m$. Por tanto $\varphi = \chi_p(\chi'\varphi) \in X_p \times \hat{U}_m$. En particular $Y \subseteq X_p \times \hat{U}_m$.

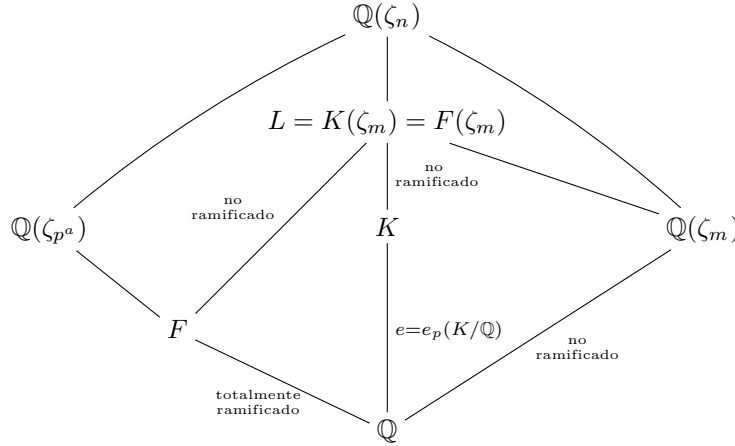
Recíprocamente, si $\xi\varphi \in X_p \times \hat{U}_m$, puesto que $\xi \in X_p$, existe $\chi \in X$ tal que $\chi_p = \xi$, es decir, $\chi = \xi \cdot \prod_{q|m} \chi_q = \xi\chi'$. Por lo tanto

$$\xi\varphi = \chi_p\varphi = \chi_p\chi'((\chi')^{-1}\varphi) \in \langle X, \hat{U}_m \rangle = Y.$$

Se sigue que $Y = X_p \times \hat{U}_m$.

Nuevamente por la Proposición 6.2.41, L se escribe como $L = \mathbb{Q}(\zeta_m)F$ donde $F \subseteq \mathbb{Q}(\zeta_n)$ es el campo perteneciente a X_p . Notemos que $F \subseteq \mathbb{Q}(\zeta_{p^a})$ pues $X_p \subseteq \hat{U}_{p^a}$.

Tenemos el siguiente diagrama donde la ramificación indicada se refiere a p :



Entonces el índice de ramificación e está dado por

$$e = e_p(K/\mathbb{Q}) = e_p(L/\mathbb{Q}) = e_p(F/\mathbb{Q}) = [F : \mathbb{Q}] = |X_p|. \quad \square$$

Como consecuencia de este resultado, tenemos:

Corolario 6.3.4. Sea χ un caracter de Dirichlet y sea K el campo asociado a X . Entonces el número primo p se ramifica en K/\mathbb{Q} si y solamente si $\chi(p) = 0$, es decir, si y solamente si $p \nmid f_\chi$.

Más generalmente, si X es un grupo de caracteres de Dirichlet y L es el campo asociado a X , entonces p se ramifica en L/\mathbb{Q} si y sólo si existe $\chi \in X$ tal que $\chi(p) = 0$, es decir, si y solamente si $p \mid f_\chi$ para algún $\chi \in X$.

Demostración. Se tiene que p se ramifica en L/\mathbb{Q} si y sólo si $X_p \neq \{1\}$, lo cual equivale a que existe $\chi \in X$ tal que $\chi_p \neq 1$. Por tanto p se ramifica en L/\mathbb{Q} si y sólo si existe $\chi \in X$ tal que $p \mid f_\chi \iff$ existe $\chi \in X$ tal que $\chi(p) = 0$. \square

El Teorema 6.3.3 se puede refinar. Se tiene

Teorema 6.3.5. Sea X un grupo de caracteres de Dirichlet y sea K su campo asociado. Sea p un número primo. Sean $Y = \{\chi \in X \mid \chi(p) \neq 0\}$ y $Z = \{\chi \in X \mid \chi(p) = 1\}$. Entonces con las notaciones usuales, tenemos

$$e = [X : Y], \quad f = [Y : Z], \quad g = [Z : 1] = |Z|.$$

Más aún, $X/Y \cong \widehat{I(\mathfrak{p}|p)}$, $X/Z \cong \widehat{D(\mathfrak{p}|p)}$, donde $I(\mathfrak{p}|p)$ y $D(\mathfrak{p}|p)$ denotan a los grupos de inercia y descomposición respectivamente de los primos en K que dividen a p .

Finalmente, el grupo de Galois de los campos residuales satisface $Y/Z \cong \widehat{\text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)}$.

Demostración. Sea L el subcampo de K que corresponde a Y . Por el Corolario 6.3.4 se tiene que L es el máximo subcampo de K en donde p es no ramificado. Por tanto, L es el campo fijo del grupo de inercia $I := I(\mathfrak{p}|p)$.

$\left. \begin{array}{c} K \\ \left\{ \right\}_{I=\text{Gal}(K/L)} \\ L \\ \left\{ \right\}_{p \text{ no ramificado}} \\ \mathbb{Q} \end{array} \right $	<p>Se tiene que $L = K^{Y^\perp}$, $Y = \text{Gal}(K/L)^\perp$. Por tanto $I \cong Y^\perp \cong \widehat{(X/Y)}$. Así $X/Y \cong \widehat{\text{Gal}(K/L)} = \hat{I}$. En particular $e = I = \hat{I} = X/Y = [X : Y]$. Ahora bien, $Y \cong \widehat{\text{Gal}(L/\mathbb{Q})}$. Sea $n := \text{mcm}\{f_\chi \mid \chi \in Y\}$. Puesto que p es no ramificado en L, $p \nmid f_\chi$ para toda $\chi \in Y$ y por tanto $p \nmid n$. Se tiene $L \subseteq \mathbb{Q}(\zeta_n)$. El automorfismo de Frobenius de p en $\mathbb{Q}(\zeta_n)$ es el automorfismo $\sigma_p: \zeta_n \rightarrow \zeta_n^p$. Por lo tanto el automorfismo de Frobenius de p en L es</p>
--	--

$$\sigma_p \text{ mód } \text{Gal}(\mathbb{Q}(\zeta_n)/L) = \overline{\sigma_p} = \sigma_p \text{ mód } H$$

donde $H := \text{Gal}(\mathbb{Q}(\zeta_n)/L)$.

Con la identificación $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U_n$, tenemos que $\overline{\sigma_p} = p \text{ mód } H$ donde consideramos $H \subseteq U_n$.

Si $\chi \in Y$, entonces $\chi(\text{Gal}(\mathbb{Q}(\zeta_n)/L)) = 1$, es decir, $\chi(H) = 1$ o, lo que es lo mismo, $H \subseteq \text{núc } \chi$. Se sigue que $\chi(\overline{\sigma_p}) = \chi(\sigma_p)$ y por lo tanto $\chi(\overline{\sigma_p}) = 1 \iff \chi(p) = 1$.

De lo anterior obtenemos que

$$\langle \overline{\sigma_p} \rangle^\perp = \{ \chi \in Y \mid \chi(p) = 1 \} = Z$$

en el mapeo bilineal

$$\text{Gal}(L/\mathbb{Q}) \times Y \longrightarrow \mathbb{C}^*.$$

Ahora bien, $\langle \overline{\sigma_p} \rangle$ es un grupo cíclico de orden f generado por $\overline{\sigma_p}$. Se sigue que

$$\frac{\widehat{\text{Gal}(L/\mathbb{Q})}}{\langle \overline{\sigma_p} \rangle^\perp} = \frac{Y}{\langle \overline{\sigma_p} \rangle^\perp} \cong \frac{Y}{Z} \cong \widehat{\langle \overline{\sigma_p} \rangle} \cong \langle \overline{\sigma_p} \rangle.$$

Por lo tanto $[Y : Z] = f = o(\overline{\sigma_p})$.

Se tiene el diagrama

$$\left. \begin{array}{c} K \\ \left| \right. \\ L \\ \left| \right. \\ E = L^{\langle \overline{\sigma_p} \rangle} \rightarrow \text{Gal}(L/E)^\perp = \langle \overline{\sigma_p} \rangle^\perp = Z \\ \left| \right. \\ \mathbb{Q} \end{array} \right\} \begin{array}{l} X/Y \rightarrow e \rightarrow \text{grupo de inercia} \\ Y/Z \rightarrow f \text{ inercia} \\ Z \rightarrow g \text{ descomposición} \end{array} \right\} X \left. \vphantom{\begin{array}{c} K \\ \left| \right. \\ L \\ \left| \right. \\ E \\ \left| \right. \\ \mathbb{Q} \end{array}} \right\} \begin{array}{l} X/Y \rightarrow ef \rightarrow \\ \rightarrow \text{grupo de descomposición} \end{array}$$

El campo fijo del automorfismo de Frobenius E corresponde al campo de descomposición de p . Por tanto E corresponde a Z y $g = [E : \mathbb{Q}] = |Z|$ o, simplemente,

$$efg = [K : \mathbb{Q}] = |X| = [X : Y][Y : Z][Z : 1] = ef[Z : 1],$$

por lo tanto $g = [Z : 1] = |Z|$. Se sigue que $X/Z \cong \widehat{D(\mathfrak{p}|p)}$. \square

6.3.1. Fórmula del Conductor–Discriminante

Nuestro objetivo en esta sección es probar que

$$|\delta_K| = \prod_{\chi \in X} f_\chi$$

donde K/\mathbb{Q} es una extensión abeliana finita y X es el grupo de caracteres de Dirichlet asociado a K .

Primero consideremos un subcampo $F \subseteq \mathbb{Q}(\zeta_{p^n})$, p con p un número primo y $n \in \mathbb{N}$. Para cualquier extensión finita K/\mathbb{Q} , denotamos por $\epsilon_K := |\delta_K|$ al valor absoluto del discriminante. Se tiene $\delta_K = (-1)^{r_2} \epsilon_K$.

Sea $p^a := \text{mcd}\{\mathfrak{f}_\varphi \mid \varphi \in X\}$ donde X es el grupo de caracteres de Dirichlet asociado a F . Entonces $F \subseteq \mathbb{Q}(\zeta_{p^a})$, $F \not\subseteq \mathbb{Q}(\zeta_{p^{a-1}})$ y $X \cong \widehat{\text{Gal}(F/\mathbb{Q})}$.

Sea $\mathfrak{P} = \langle 1 - \zeta_{p^a} \rangle$ el único ideal en $\mathcal{O}_{\mathbb{Q}(\zeta_{p^a})} = \mathbb{Z}[\zeta_{p^a}]$ sobre p y sea $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_F$.

Empezamos analizando los grupos de ramificación de $\mathbb{Q}(\zeta_{p^a})$. Sea $G := \text{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$. Se tiene $(p)\mathcal{O}_{\mathbb{Q}(\zeta_{p^a})} = \mathfrak{P}^{\varphi(p^a)} = (\zeta_{p^a} - 1)^{\varphi(p^a)}$. Sea $\sigma \in G$, $\sigma \neq 1$, dado por $\sigma(\zeta_{p^a}) = \zeta_{p^a}^{a_\sigma}$, $a_\sigma \in \mathbb{Z}$, $1 \leq a_\sigma \leq p^a - 1$, $\text{mcd}(a_\sigma, p) = 1$. Sea $a_\sigma - 1 = p^{\alpha_\sigma} \ell_\sigma$ con $\text{mcd}(\ell_\sigma, p) = 1$, $0 \leq \alpha_\sigma \leq a - 1$. Entonces

$$\begin{aligned} i_G(\sigma) &:= v_{\mathfrak{P}}(\sigma(\zeta_{p^a}) - \zeta_{p^a}) = v_{\mathfrak{P}}(\zeta_{p^a}^{a_\sigma} - \zeta_{p^a}) = v_{\mathfrak{P}}(\zeta_{p^a}^{a_\sigma} (\zeta_{p^a}^{a_\sigma - 1} - 1)) \\ &= v_{\mathfrak{P}}(\zeta_{p^a}^{p^{\alpha_\sigma} \ell_\sigma} - 1) = v_{\mathfrak{P}}(\zeta_{p^{n-\alpha_\sigma}}^{\ell_\sigma} - 1) = v_{\mathfrak{P}}(\zeta_{p^{n-\alpha_\sigma}} - 1) \\ &= v_{\mathfrak{P}}((\zeta_{p^a} - 1)^{p^{\alpha_\sigma}}) = p^{\alpha_\sigma}. \end{aligned}$$

Es decir,

$$i_G(\sigma) = p^{\alpha_\sigma}. \quad (6.1)$$

Se tiene que $\sigma \in G_u \iff v_{\mathfrak{P}}(\sigma(\zeta_{p^a}) - \zeta_{p^a}) = p^{\alpha_\sigma} \geq u + 1 \iff u \leq p^{\alpha_\sigma} - 1$. Se sigue que

$$G_u = \{\sigma \in G \mid \sigma(\zeta_{p^a}) = \zeta_{p^a}^{a_\sigma}, v_p(a_\sigma - 1) = \alpha_\sigma, u \leq p^{\alpha_\sigma} - 1\}. \quad (6.2)$$

De (6.2) y recordando que $D_{p^a, p^m} = \text{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}(\zeta_{p^m}))$, $1 \leq m \leq a$, $D_{p^a, p^0} = D_{p^n, 1} = G$, se tiene que

$$\begin{aligned} G_{-1} &= G_0 = G, \\ G_u &\cong D_{p^a, p}, & 1 \leq u \leq p - 1, \\ G_u &\cong D_{p^a, p^2}, & p \leq u \leq p^2 - 1, \\ &\vdots & \vdots \\ G_u &\cong D_{p^a, p^{a-1}}, & p^{a-2} \leq p^{a-1} - 1, \\ G_u &= \{1\}, & p^{a-1} \leq u. \end{aligned}$$

Como consecuencia del Teorema 1.3.5 se tiene que se $\mathfrak{D}_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}} = \mathfrak{P}^s$, entonces

$$\begin{aligned} s &= \sum_{j=0}^{\infty} (|G_j| - 1) = (|G| - 1) + \sum_{j=1}^{a-1} (p^j - p^{j-1})(|D_{p^a, p^j}| - 1) \\ &= [\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] - 1 + \sum_{j=1}^{a-1} [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}] ([\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}(\zeta_{p^j})] - 1) \\ &= a[\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] - \sum_{j=0}^{a-1} [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]. \end{aligned}$$

Notemos que

$$\begin{aligned} s &= a\varphi(p^a) - \sum_{j=0}^{a-1} \varphi(p^j) = a(p^{a-1}(p-1)) - \sum_{j=1}^{a-1} (p^j - p^{j-1}) - 1 \\ &= ap^a - ap^{a-1} - p^{a-1} + 1 - 1 = p^{a-1}(ap - a - 1), \end{aligned}$$

lo cual nos da una nueva demostración del Corolario 3.2.27.

Para el caso en que $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_{p^a})$, sea $F_j := F \cap \mathbb{Q}(\zeta_{p^j})$, $0 \leq j \leq a$. Sea $H := \text{Gal}(\mathbb{Q}(\zeta_{p^a})/F)$ y sea $\mathfrak{D}_{\mathbb{Q}(\zeta_{p^a})/F} = \mathfrak{P}^t$. Se tiene que $G_j \cong D_{p^a, p^{r_j}}$ para alguna r_j . Por la Proposición 1.3.7 se tiene que $H_j = G_j \cap H = \text{Gal}(\mathbb{Q}(\zeta_{p^a})/E\mathbb{Q}(\zeta_{p^{r_j}}))$. Por lo tanto

$$\begin{aligned} t &= \sum_{\sigma \in H \setminus \{1\}} i_H(\sigma) = \sum_{\sigma \in H \setminus \{1\}} i_G(\sigma) = \sum_{j=0}^{\infty} (|H_j| - 1) = \sum_{j=0}^{\infty} (|G_j \cap H| - 1) \\ &= ([\mathbb{Q}(\zeta_{p^a}) : F] - 1) + \sum_{j=1}^{a-1} [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}] ([\mathbb{Q}(\zeta_{p^a}) : F\mathbb{Q}(\zeta_{p^j})] - 1). \end{aligned}$$

Puesto que

$$\mathfrak{D}_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}} = \mathfrak{D}_{\mathbb{Q}(\zeta_{p^a})/F} \cdot \text{con}_{F/\mathbb{Q}(\zeta_{p^a})} \mathfrak{D}_{F/\mathbb{Q}}, \quad (6.3)$$

y \mathfrak{p} es totalmente ramificado en $\mathbb{Q}(\zeta_{p^a})/F$, se tiene que si $\mathfrak{D}_{F/\mathbb{Q}} = \mathfrak{p}^r$, entonces de (6.3) se obtiene que $\mathfrak{P}^s = \mathfrak{P}^t \mathfrak{P}^{r[\mathbb{Q}(\zeta_{p^a}) : F]}$, esto es

$$\begin{aligned} r &= \frac{s-t}{[\mathbb{Q}(\zeta_{p^a}) : F]} = \frac{1}{[\mathbb{Q}(\zeta_{p^a}) : F]} \left\{ ([\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] - [\mathbb{Q}(\zeta_{p^a}) : F] \right. \\ &\quad \left. + \sum_{j=1}^{a-1} [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}] ([\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}(\zeta_{p^j})] - [\mathbb{Q}(\zeta_{p^a}) : F\mathbb{Q}(\zeta_{p^j})]) \right\} \\ &= ([F : \mathbb{Q}] - 1) + \frac{1}{[\mathbb{Q}(\zeta_{p^a}) : F]} \\ &\quad \left\{ \sum_{j=1}^{a-1} ([\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] - [\mathbb{Q}(\zeta_{p^a}) : F\mathbb{Q}(\zeta_{p^j})] \cdot [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]) \right\}. \end{aligned}$$

Se sigue que

$$\begin{aligned} r &= [F : \mathbb{Q}] - 1 + \sum_{j=1}^{a-1} \left([F : \mathbb{Q}] - \frac{[\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]}{[F\mathbb{Q}(\zeta_{p^j}) : F]} \right) \\ &= a[F : \mathbb{Q}] - \sum_{j=0}^{a-1} \frac{[\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]}{[F\mathbb{Q}(\zeta_{p^j}) : F]}. \end{aligned}$$

Ahora bien, se tiene

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_{p^j}) & \xrightarrow{\quad\quad\quad} & F\mathbb{Q}(\zeta_{p^j}) & [F\mathbb{Q}(\zeta_{p^j}) : F] = [\mathbb{Q}(\zeta_{p^j}) : F_j], \\
\downarrow & & \downarrow & \\
F_j = \mathbb{Q}(\zeta_{p^j}) \cap F & \xrightarrow{\quad\quad\quad} & F &
\end{array}$$

por lo que

$$\frac{[\mathbb{Q}(\zeta_{p^j}); \mathbb{Q}]}{[F\mathbb{Q}(\zeta_{p^j}) : F]} = \frac{[\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{p^j}) : F_j]} = [F_j : \mathbb{Q}].$$

Se sigue que

$$r = a[F : \mathbb{Q}] - \sum_{j=0}^{a-1} [F_j : \mathbb{Q}]. \quad (6.4)$$

Hemos probado

Proposición 6.3.6. *Sea $Q \subseteq F \subseteq \mathbb{Q}(\zeta_{p^a})$, $p \geq 2$ un número primo y $a \geq 1$. Entonces $\mathfrak{D}_{F/\mathbb{Q}} = \mathfrak{p}^r$, donde $r = a[F : \mathbb{Q}] - \sum_{j=0}^{a-1} [F_j : \mathbb{Q}]$. \square*

Corolario 6.3.7. *Con las condiciones anteriores, $|\mathfrak{D}_{F/\mathbb{Q}}| = p^r$. \square*

Ahora bien, sea X el grupo de caracteres de Dirichlet asociado a F . Se tiene que $F_a = F$ y $F_0 = \mathbb{Q}$. Un caracter χ tiene conductor p^j si y solamente si χ es un caracter asociado a $\mathbb{Q}(\zeta_{p^j})$ pero no asociado a $\mathbb{Q}(\zeta_{p^{j-1}})$. Por lo tanto X contiene precisamente $[F_j : \mathbb{Q}] - [F_{j-1} : \mathbb{Q}]$ caracteres de conductor p^j , $1 \leq j \leq a$. Se sigue que $\prod_{\chi \in X} \mathfrak{f}_\chi = p^\alpha$ donde

$$\alpha = \sum_{j=1}^a j([F_j : \mathbb{Q}] - [F_{j-1} : \mathbb{Q}]) = n[F : \mathbb{Q}] - \sum_{j=0}^{a-1} [F_j : \mathbb{Q}]. \quad (6.5)$$

De (6.4) y (6.5) se sigue

Proposición 6.3.8. *Si $F \subseteq \mathbb{Q}(\zeta_{p^a})$ con p un número primo, y X es el grupo de caracteres de Dirichlet asociado a F , entonces*

$$\epsilon_F = \prod_{\chi \in X} \mathfrak{f}_\chi. \quad \square$$

Teorema 6.3.9 (fórmula del conductor–discriminante). *Sea K/\mathbb{Q} una extensión abeliana finita. Entonces*

$$\delta_K = (-1)^{r_2} \prod_{\chi \in X} \mathfrak{f}_\chi$$

donde X denota el grupo de caracteres de Dirichlet asociado a K .

Demostración. Basta probar que $\epsilon_K = \prod_{\chi \in X} \mathfrak{f}_\chi$. Fijemos un número primo p . Con las notaciones del Teorema 6.3.3, tenemos que puesto que ningún primo encima de p es ramificado ni en L/K ni en L/F y puesto que

$$\mathfrak{D}_{L/\mathbb{Q}} = \mathfrak{D}_{L/K} \cdot \text{con}_{K/L} \mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{L/F} \cdot \text{con}_{F/L} \mathfrak{D}_{F/\mathbb{Q}}, \quad (6.6)$$

se tiene que si para cualquier extensión M/\mathbb{Q} , $\mathfrak{d}_{M/\mathbb{Q}}(p)$ denota la potencia exacta de $\langle p \rangle$ que divide a $\mathfrak{d}_{M/\mathbb{Q}}$ (y similarmente para $\epsilon_M(p)$), entonces de (6.6)

$$\mathfrak{d}_{L/\mathbb{Q}}(p) = (N_{L/\mathbb{Q}} \mathfrak{D}_{L/\mathbb{Q}})(p) = \mathfrak{d}_{K/\mathbb{Q}}^{[L:K]}(p) = \mathfrak{d}_{F/\mathbb{Q}}^{[L:F]}(p).$$

Por lo tanto

$$\epsilon_K(p) = \epsilon_L^{(1/[L:K])}(p) = \epsilon_F^{([L:F]/[L:K])}(p).$$

Ahora bien $[L : F] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ y $[L : K] = [Y : X] = \frac{|Y|}{|X|} = \frac{|X_p| |\hat{\mathcal{U}}_m|}{|X|} = \frac{|X_p| \varphi(m)}{|X|}$. Se sigue que $\frac{[L:F]}{[L:K]} = \frac{|X|}{|X_p|}$. Puesto que $F \subseteq \mathbb{Q}(\zeta_{p^a})$, obtenemos de la Proposición 6.3.8 que $\epsilon_F = \prod_{\varphi \in X_p} \mathfrak{f}_\varphi$. Por tanto

$$\epsilon_K(p) = \epsilon_F^{(|X|/|X_p|)}(p) = \left(\prod_{\varphi \in X_p} \mathfrak{f}_\varphi \right)^{|X|/|X_p|}.$$

Del epimorfismo natural $\pi: X \rightarrow X_p$, $\chi \mapsto \chi_p$, obtenemos que $|\text{nuc } \pi| = \frac{|X|}{|X_p|}$. Del Teorema 6.3.3, $|X_p| = e$ y $|X| = [K : \mathbb{Q}] = efg$ (con las notaciones usuales). Entonces, cada χ_p aparece para exactamente $fg = \frac{|X|}{|X_p|}$ elementos diferentes de X , esto es, $|\pi^{-1}(\chi_p)| = fg$. Por lo tanto

$$\epsilon_K(p) = \left(\prod_{\varphi \in X_p} \mathfrak{f}_\varphi \right)^{fg} = \prod_{\chi \in X} \mathfrak{f}_{\chi_p}.$$

Puesto que $\epsilon_K = \prod_p \epsilon_K(p)$, tenemos

$$\epsilon_K = \prod_p \epsilon_K(p) = \prod_p \prod_{\chi \in X} \mathfrak{f}_{\chi_p} = \prod_{\chi \in X} \prod_p \mathfrak{f}_{\chi_p}.$$

Finalmente, puesto que para cualesquiera dos primos diferentes p y q , \mathfrak{f}_{χ_p} y \mathfrak{f}_{χ_q} son primos relativos y $\chi = \prod_p \chi_p$, se sigue del Teorema 6.2.25 que $\mathfrak{f}_\chi = \prod_p \mathfrak{f}_{\chi_p}$, así que:

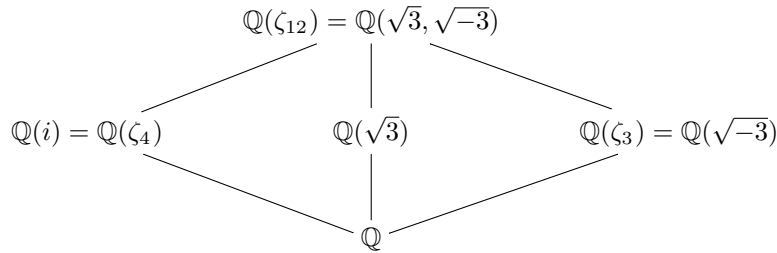
$$\epsilon_K = \prod_p \epsilon_K(p) = \prod_{\chi \in X} \prod_p \mathfrak{f}_{\chi_p} = \prod_{\chi \in X} \mathfrak{f}_\chi. \quad \square$$

6.4. Construcción de extensiones abelianas

El Teorema 6.3.3 es muy útil para construir extensiones abelianas con características especiales. Primero veamos como funciona con un ejemplo específico.

Ejemplo 6.4.1. Consideremos el caracter cuadrático $\chi: U_{12} \rightarrow \mathbb{C}^*$ dado por $\chi(1) = \chi(11) = 1$ y $\chi(5) = \chi(7) = -1$. Entonces el caracter es real, $f_\chi = 12$ y el campo asociado tiene que ser $\mathbb{Q}(\zeta_{12})^+ = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1}) = \mathbb{Q}(\sqrt{3})$.

Sea $\chi = \chi_2 \chi_3$. Entonces $f_{\chi_2} = 4$ y $f_{\chi_3} = 3$. Por tanto los campos asociados a χ_2 y χ_3 son $\mathbb{Q}(\zeta_4)$ y $\mathbb{Q}(\zeta_3)$ respectivamente. Sea $Y = \langle \chi_2 \rangle \times \langle \chi_3 \rangle$. Se tiene que el campo asociado a Y es $\mathbb{Q}(\zeta_4)\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_{12})$. En particular $Y = \widehat{U_{12}}$. Se tiene



Notemos que la ramificación está dada por:

- (I) En $\mathbb{Q}(\zeta_4)/\mathbb{Q}$: 2 y el primo infinito ∞ .
- (II) En $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$: 2 y 3.
- (III) En $\mathbb{Q}(\zeta_3)/\mathbb{Q}$: 3 e ∞ .
- (IV) En $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)$: 3.
- (V) En $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\sqrt{3})$: ∞ .
- (VI) En $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3)$: 2.

En particular $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\sqrt{3})$ es no ramificada en ningún primo finito.

6.4.1. Campos de géneros

Teorema 6.4.2 (Leopoldt [45]). Sea K/\mathbb{Q} una extensión abeliana finita. Se L la máxima extensión abeliana de \mathbb{Q} que es no ramificada en ningún primo finito. Entonces el grupo de caracteres de Dirichlet Y correspondiente a L es

$$Y = \prod_p X_p$$

donde X es el grupo de caracteres de Dirichlet correspondiente a K .

Demostración. Primero notemos que para todo número primo p , $Y_p = X_p$ y por tanto $|Y_p| = |X_p|$. Por el Teorema 6.3.3 se sigue que $e_p(L/K) = 1$ y L/K es no ramificada en ningún primo finito.

Ahora, sea E/K una extensión no ramificada en ningún primo finito y E/\mathbb{Q} abeliana. Sea Z el grupo de caracteres de Dirichlet asociado a E . Entonces $|X_p| = |Z_p|$ y $Z \supseteq X$. Por lo tanto $Z_p = X_p$ y se sigue que $Z \subseteq \prod_p Z_p = \prod_p X_p = Y$ y por lo tanto $E \subseteq L$. \square

Supongamos que L/K es ramificada en los primos infinitos. Entonces $K \subseteq \mathbb{R}$ y $L \not\subseteq \mathbb{R}$. Sea $Y^+ := \{\chi \in Y \mid \chi(-1) = 1\}$. Puesto que para toda $\chi \in X$, $\chi(-1) = 1$, $X \subseteq Y^+$. Por otro lado $Y^+ = \text{nuc } \theta$ donde $\theta: Y \rightarrow \{\pm 1\}$, $\theta(\chi) = \chi(-1)$ y puesto que $L \not\subseteq \mathbb{R}$, existe $\chi \in Y$ con $\chi(-1) = -1$, es decir, θ es una función suprayectiva. Se sigue que $Y/Y^+ \cong \{\pm 1\}$ y en particular $|Y^+| = |Y|/2$.

Corolario 6.4.3. *Con las notaciones del Teorema 6.4.2 se tiene que si L^+ es el campo correspondiente a Y^+ , entonces*

- (1) *Si K y L son ambos reales o ambos imaginarios, L es la máxima extensión de K y abeliana sobre \mathbb{Q} , no ramificada en todo primo incluyendo los primos infinitos.*
- (2) *Si K es real y L es imaginario, L^+/K es la máxima extensión no ramificada en ningún primo incluyendo los primos infinitos y abeliana sobre \mathbb{Q} . Ahora, L/K es la máxima extensión no ramificada en ningún primo finito y abeliana sobre \mathbb{Q} .* \square

Ejemplo 6.4.4. En el Ejemplo 6.4.1, $K = \mathbb{Q}(\sqrt{3})$ con $X = \{\chi\}$, $\chi: U_{12} \rightarrow \mathbb{C}^*$, $\chi(1) = \chi(11) = 1$, $\chi(5) = \chi(7) = -1$, $Y = \langle \chi_2 \rangle \times \langle \chi_3 \rangle$ y $Y = \widehat{U_{12}}$, $Y^+ = X$. Por tanto toda extensión L/K , L/\mathbb{Q} abeliana, es ramificada en algún primo.

Ejemplo 6.4.5. Sea p un primo impar y sea $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subseteq \mathbb{Q}(\zeta_p)$ la subextensión cuadrática de $\mathbb{Q}(\zeta_p)$. Sea $\chi: U_p \rightarrow \mathbb{C}^*$ el caracter asociado a K , $X = \langle \chi \rangle$. Entonces $o(\chi) = 2 = [K : \mathbb{Q}]$, $\chi^2 = 1$ y $\chi \neq 1$. El conductor de χ es $f_\chi = p$. Se tiene $\chi(U_p) = \{\pm 1\}$. Ahora bien, $K = \mathbb{Q}(\zeta_p)^{\text{nuc } \chi}$ con

$$\text{nuc } \chi = \{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \mid \chi(\sigma) = 1\}.$$

Sea q cualquier número primo, $q \neq p$. Se tiene que q se descompone en K/\mathbb{Q} si y sólo si $|Z| = 2$ en la notación del Teorema 6.3.5, es decir, $Z = \{\varphi \in X \mid \varphi(q) = 1\}$. Esto es, q se descompone en $K/\mathbb{Q} \iff \chi(q) = 1$.

Por otro lado, si $q \equiv a^2 \pmod{p}$ para algún $a \in \mathbb{Z}$, entonces $\chi(q) = \chi(a)^2 = 1$ y puesto que

$$|\text{nuc } \chi| = \frac{|U_p|}{2} = \frac{p-1}{2} = |\{t \in U_p \mid t \equiv a^2 \pmod{p}\}|$$

se sigue que $\chi(q) = 1 \iff q \equiv a^2 \pmod{p} \iff \left(\frac{q}{p}\right) = 1$ donde $\left(\frac{q}{p}\right)$ es el símbolo de Legendre. Por tanto $\chi(q) = \left(\frac{q}{p}\right)$.

En resumen, el campo $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ corresponde al símbolo de Legendre: $\chi(q) = \left(\frac{q}{p}\right)$.

Ejemplo 6.4.6. Con respecto al Ejemplo 6.4.5, nos preguntamos ahora cual es el caracter cuadrático de Dirichlet correspondiente al campo cuadrático $\mathbb{Q}(\sqrt{(-1)^{(p+1)/2}p})$ donde p es un número primo impar.

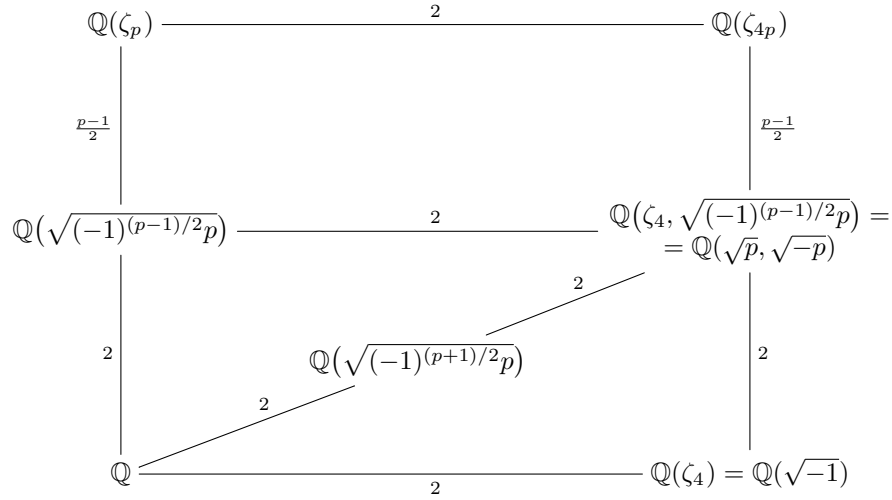
Recordemos que si $p \equiv 1 \pmod{4}$, entonces

$$\sqrt{(-1)^{(p-1)/2}p} = \sqrt{p} \quad \text{y} \quad \sqrt{(-1)^{(p+1)/2}p} = \sqrt{-p}$$

y si $p \equiv 3 \pmod{4}$ entonces

$$\sqrt{(-1)^{(p-1)/2}p} = \sqrt{-p} \quad \text{y} \quad \sqrt{(-1)^{(p+1)/2}p} = \sqrt{p}.$$

Tenemos el siguiente diagrama



Sean

$$\begin{aligned} \chi: U_p &\longrightarrow \mathbb{C}^*, & \chi(q) &= \left(\frac{q}{p}\right), \\ \varphi: U_4 &\longrightarrow \mathbb{C}^*, & \varphi(-1) &= -1. \end{aligned}$$

$$\text{Por tanto } \varphi(q) = \begin{cases} 1 & \text{si } q \equiv 1 \pmod{4} \\ -1 & \text{si } q \equiv -1 \pmod{4} \equiv 3 \pmod{4} \end{cases} = (-1)^{(q-1)/2}.$$

Se sigue que $\mathbb{Q}(\sqrt{(-1)^{(p+1)/2}p})$ corresponde a $\varphi\chi$ el cual está definido por $(\varphi\chi)(q) = (-1)^{(q-1)/2} \left(\frac{q}{p}\right)$.

Finalmente, notemos que $f_{\varphi\chi} = f_{\varphi}f_{\chi} = 4p$ y que $\epsilon_{\mathbb{Q}(\sqrt{(-1)^{(p+1)/2}p})} = |\delta_{\mathbb{Q}(\sqrt{(-1)^{(p+1)/2}p})}| = 4p$.

Ejemplo 6.4.7. Sea $K_1 = \mathbb{Q}(\sqrt{10})$. Entonces $K_1 = \mathbb{Q}(\sqrt{10}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5}) \subseteq \mathbb{Q}(\zeta_8, \zeta_5) = \mathbb{Q}(\zeta_{40})$ pues $5 \equiv 1 \pmod{4}$. Además $\text{Gal}(\mathbb{Q}(\zeta_{40})/\mathbb{Q}) \cong U_{40} \cong U_8 \times U_5 \cong (C_2 \times C_2) \times C_4 = G$.

$$\begin{array}{c} \mathbb{Q}(\zeta_8) \\ | \\ \mathbb{Q} \text{ ————— } \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5)^+ \text{ ————— } \mathbb{Q}(\zeta_5) \end{array}$$

G tiene 7 subgrupos de orden 2 y por tanto 7 grupos cociente de índice 2. Se sigue que $\mathbb{Q}(\zeta_{40})$ tiene 7 subcampos cuadráticos:

$$\mathbb{Q}(\zeta_4), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{10}) \text{ y } \mathbb{Q}(\sqrt{-10}).$$

Puesto que $\mathbb{Q}(\sqrt{10}) \not\subseteq \mathbb{Q}(\zeta_4), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{10}), \mathbb{Q}(\zeta_{20})$ se sigue que el caracter χ asociado a $\mathbb{Q}(\sqrt{10})$ tiene conductor $f_{\chi} = 40$ (o simplemente porque $\delta_{\mathbb{Q}(\sqrt{10})} = 40 = f_{\chi}$).

Se sigue que $\chi = \chi_2\chi_5$, $f_{\chi_2} = 8$, $f_{\chi_5} = 5$. Además $\chi(-1) = 1$ por lo que $\chi_2(-1) = \chi_5(-1) = \pm 1$. En caso de que $\chi_2(-1) = \chi_5(-1) = -1$ se tendría que $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\zeta_5)$ pues $\chi_5(-1) = -1$ significa que el subcampo cuadrático de $\mathbb{Q}(\zeta_5)$ sería complejo. Se sigue que $\chi_2(-1) = \chi_5(-1) = 1$ y $\chi_2^2 = \chi_5^2 = 1$. Por lo tanto $\mathbb{Q}(\sqrt{2})$ es el campo asociado a χ_2 y $\mathbb{Q}(\sqrt{5})$ es el campo asociado a χ_5 .

Si $Y = \langle \chi_2 \rangle \oplus \langle \chi_5 \rangle$ entonces el campo asociado a Y es $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ y $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es la máxima extensión abeliana de \mathbb{Q} no ramificada sobre $\mathbb{Q}(\sqrt{10})$ pues ∞ es no ramificado debido a que $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es un campo real.

Ahora bien, usando el campo de clase de Hilbert (ver Teorema 1.4.3), esto es, si H_K es la máxima extensión abeliana de K no ramificada en ningún primo incluyendo el ∞ , se tiene que $C_K \cong \text{Gal}(H_K/K)$ donde C_K es el grupo de clases de K . Puesto que $L \subseteq H_K$, $2 = [L : K][H_K : K] = |C_K| = h_K$, es decir, $2|h_K$ y K , más precisamente, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{10}}{2}]$, no es de ideales principales.

Ejemplo 6.4.8. Sea ahora $K = \mathbb{Q}(\sqrt{-5})$. Se tiene $5 \equiv 1 \pmod{4}$ y por lo tanto $\mathbb{Q}(\sqrt{-5}) \not\subseteq \mathbb{Q}(\zeta_5)$ y $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{5}) \subseteq \mathbb{Q}(\zeta_4, \zeta_5) = \mathbb{Q}(\zeta_{20})$ y se tiene $\text{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong U_{20} \cong U_4 \times U_5 \cong C_2 \times C_4$. En particular $\mathbb{Q}(\zeta_{20})$ tiene tres subcampos cuadráticos, a saber, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{5})$ y $\mathbb{Q}(\sqrt{-5})$. Puesto que $\delta_K = -20$, $f_{\chi} = 20$ donde χ es el caracter asociado a K .

Sea $\chi = \chi_2\chi_5$ con $f_{\chi_2} = 4$ y $f_{\chi_5} = 5$. Puesto que $\chi(-1) = -1$ y $\chi_2(-1) \neq \chi_5(-1)$. Más precisamente, únicamente hay un caracter cuadrático de conductor 4, el correspondiente a $\mathbb{Q}(\zeta_4)$, y un único caracter cuadrático módulo 5, el correspondiente a $\mathbb{Q}(\sqrt{5})$. Por tanto se tiene $\chi_2(-1) = -1$ y $\chi_5(-1) = 1$. Así, el campo asociado a $Y = \langle \chi_2 \rangle \oplus \langle \chi_5 \rangle$ es $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ el cual es la máxima extensión abeliana de \mathbb{Q} no ramificada en ningún primo sobre K , incluyendo al primo infinito pues K es un campo complejo.

Similarmente a como en el Ejemplo 6.4.7, se tiene que $2|h_K$ y $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ no es de ideales principales.

Ejemplo 6.4.9. Sea ahora $K = \mathbb{Q}(\sqrt{30})$. Se tiene $30 = 2 \cdot 3 \cdot 5$, $\delta_K = 4 \cdot 30 = 120$ por lo que el conductor de χ , el caracter asociado a K , es igual a $f_\chi = 120$. Ahora bien

$$\mathbb{Q}(\sqrt{30}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\zeta_8, \zeta_{12}, \zeta_5) = \mathbb{Q}(\zeta_8, \zeta_3, \zeta_5) = \mathbb{Q}(\zeta_{120}).$$

Además

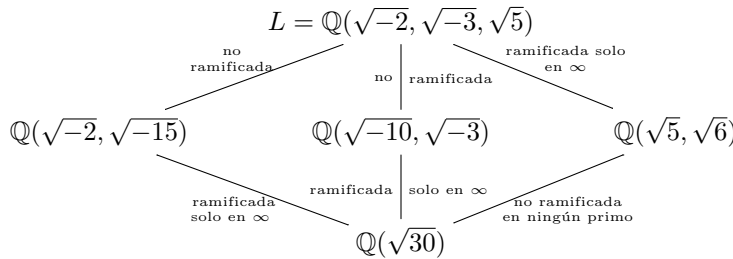
$$\text{Gal}(\mathbb{Q}(\zeta_{120})/\mathbb{Q}) \cong U_{120} \cong U_8 \times U_3 \times U_5 \cong (C_2 \times C_2) \times (C_2) \times (C_4).$$

En particular $\mathbb{Q}(\zeta_{120})$ tiene $\frac{2^4-1}{2-1} = 15$ subcampos cuadráticos. Sea $\chi = \chi_2\chi_3\chi_5$, $f_{\chi_2} = 8$, $f_{\chi_3} = 3$, $f_{\chi_5} = 5$ y $\chi_2^2 = \chi_3^2 = \chi_5^2 = 1$. Puesto que únicamente existen un caracter cuadrático de conductores 3 y 5 respectivamente, χ_3 corresponde a $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, y χ_5 corresponde a $\mathbb{Q}(\sqrt{5})$. Además $\chi_3(-1) = -1$ y $\chi_5(-1) = 1$. Puesto que $\chi(-1) = 1$, se tiene que $\chi_2(-1) = -1$ y por tanto χ_2 corresponde a $\mathbb{Q}(\sqrt{-2})$.

Sea $Y = \langle \chi_2 \rangle \oplus \langle \chi_3 \rangle \oplus \langle \chi_5 \rangle$. Entonces el campo L asociado a Y es $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{5})$.

Notemos K es real y L es imaginario, por lo que los primos infinitos de K son ramificados en L . Sea $Y^+ = \{\varphi \in Y \mid \varphi(-1) = 1\}$, Y^+ corresponde a $L^+ = L \cap \mathbb{R}$. Entonces $Y^+ = \langle \chi_2\chi_3 \rangle \oplus \langle \chi_5 \rangle$ y $\chi_2\chi_3$ corresponde a $\mathbb{Q}(\sqrt{-2}\sqrt{-3}) = \mathbb{Q}(\sqrt{6})$. Por lo tanto $L^+ = \mathbb{Q}(\sqrt{6}, \sqrt{5})$ y L^+ es la máxima extensión abeliana de \mathbb{Q} no ramificada en ningún primo de K incluyendo al infinito.

Por otro lado $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{5})$ es la máxima extensión abeliana de \mathbb{Q} no ramificada en ningún primo finito de K .



Los Ejemplos 6.4.7, 6.4.8 y 6.4.9 nos dan la guía del caso general que a continuación estudiamos.

Ejemplo 6.4.10. Sean $d \in \mathbb{Z}$ libre de cuadrados, $K = \mathbb{Q}(\sqrt{d})$. Escribamos $d = (-1)^\varepsilon 2^\delta p_1 \cdots p_s q_1 \cdots q_t$ donde $\varepsilon, \delta \in \{0, 1\}$, p_1, \dots, p_s primos distintos congruentes con 1 módulo 4 y q_1, \dots, q_t primos distintos congruentes con 3 módulo 4.

Sea χ el caracter cuadrático asociado a K . Se tiene que

$$f_\chi = |\delta_K| = \begin{cases} |d| & \text{si } d \equiv 1 \pmod{4} \\ 4|d| & \text{si } d \equiv 2, 3 \pmod{4} \end{cases}.$$

Por el Ejemplo 6.4.5 se tiene que χ_{p_i}, χ_{q_j} corresponden al símbolo de Legendre: $\chi_{p_i}(\ell) = \left(\frac{\ell}{p_i}\right)$, $\chi_{q_j}(\ell) = \left(\frac{\ell}{q_j}\right)$, $1 \leq i \leq s$, $1 \leq j \leq t$. Además $\chi_{p_i}(-1) = 1$, $i = 1, 2, \dots, s$ y $\chi_{q_j}(-1) = -1$, $j = 1, 2, \dots, t$. Por otro lado χ_{p_i} corresponde al campo $\mathbb{Q}(\sqrt{(-1)^{(p_i-1)/2} p_i}) = \mathbb{Q}(\sqrt{p_i})$, $1 \leq i \leq s$ y χ_{q_j} corresponde al campo $\mathbb{Q}(\sqrt{(-1)^{(q_j-1)/2} q_j}) = \mathbb{Q}(\sqrt{-q_j})$, $1 \leq j \leq t$.

Más aún $\chi(-1) = (-1)^\varepsilon$. El problema más complicado es ver que es χ_2 . Se tiene

$$d \equiv (-1)^\varepsilon 2^\delta (-1)^t \pmod{4} \equiv (-1)^{\varepsilon+t} 2^\delta \pmod{4}.$$

Por tanto

$$\begin{aligned} d \equiv 1 \pmod{4} &\iff \delta = 0 \text{ y } \varepsilon + t \text{ es par,} \\ d \equiv 2 \pmod{4} &\iff \delta = 1, \\ d \equiv 3 \pmod{4} &\iff \delta = 0 \text{ y } \varepsilon + t \text{ es impar.} \end{aligned}$$

Ahora si $d \equiv 1 \pmod{4}$, $f_{\chi_2} = 1$. Si $d \equiv 2 \pmod{4}$, entonces $f_{\chi_2} = 8$ y χ_2 puede corresponder a $\mathbb{Q}(\sqrt{2})$ o a $\mathbb{Q}(\sqrt{-2})$. Si $d \equiv 3 \pmod{4}$, entonces $f_{\chi_2} = 4$ y χ_2 corresponde a $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ y $\chi_2(-1) = -1$.

Veamos todos los casos:

(i) Si $d \equiv 1 \pmod{4}$,

(a) K es real, $d > 0$. En este caso $\varepsilon = 0$, $\delta = 0$, t es par. Se tiene que

$$Y = \left(\bigoplus_{i=1}^s \langle \chi_{p_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \langle \chi_{q_j} \rangle \right).$$

El campo L correspondiente a Y será:

$$L = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}).$$

Si $t > 0$, L es imaginario y entonces

$$Y^+ = \left(\bigoplus_{i=1}^s \langle \chi_{p_i} \rangle \right) \oplus \left(\bigoplus_{j=2}^t \langle \chi_{q_1} \chi_{q_j} \rangle \right).$$

y el campo asociado a Y^+ es

$$\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_t}).$$

Notemos que $2^{s+t-2} | h_K$.

- (b) Si K es imaginario, $d < 0$, $\varepsilon = 1$, t es impar y $L = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t})$
 Notemos que $2^{s+t-1} | h_K$.

- (II) Si $d \equiv 2 \pmod{4}$. Se tiene que $f_{\chi_2} = 8$ en este caso y

$$Y = \langle \chi_2 \rangle \oplus \left(\bigoplus_{i=1}^s \langle \chi_{p_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \langle \chi_{q_j} \rangle \right).$$

Además $(-1)^\varepsilon = \chi(-1) = \chi_2(-1)(-1)^t$. Por tanto $\chi_2(-1) = (-1)^{t+\varepsilon}$.

- (a) Si K es real, $d > 0$, $\varepsilon = 0$, $\chi_2(-1) = (-1)^t$. Si t es par, $\chi_2(-1) = 1$ y χ_2 corresponde a $\mathbb{Q}(\sqrt{2})$. Si t es impar, χ_2 corresponde a $\mathbb{Q}(\sqrt{-2})$. Se tiene

$$L = \mathbb{Q}(\sqrt{(-1)^t 2}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}).$$

Si $t = 0$, $L^+ = L = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_s})$ y $2^s | h_K$.

Si $t > 0$, t par,

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}),$$

$$L^+ = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_t}) \quad \text{y} \quad 2^{s+t-1} | h_K.$$

Si t es impar,

$$L = \mathbb{Q}(\sqrt{-2}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}),$$

$$L^+ = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{2q_1}, \dots, \sqrt{2q_t}) \quad \text{y} \quad 2^{s+t-1} | h_K.$$

- (b) Si K es imaginario, $d < 0$, $\varepsilon = 1$, $\chi_2(-1) = (-1)^{t+1}$ por lo que χ_2 corresponde a $\mathbb{Q}(\sqrt{(-1)^{t+1} 2})$. Se tiene

$$L = \mathbb{Q}(\sqrt{(-1)^{t+1} 2}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t})$$

y $2^{s+t} | h_K$.

- (III) $d \equiv 3 \pmod{4}$. En este caso $f_\chi = 4$ y por tanto $\chi(-1) = -1$ y χ_2 corresponde a $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$.

- (a) si K es real, $d > 0$, $\varepsilon = 0$, $\chi_2(-1) = -1$ y $\chi(-1) = (-1)^\varepsilon = 1 = \chi_2(-1) \prod_{j=1}^t \chi_{q_j}(-1) = (-1)^{1+t}$. Por lo tanto t es impar. Entonces

$$L = \mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}),$$

$$L^+ = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{q_1}, \dots, \sqrt{q_t}) \quad \text{y} \quad 2^{s+t-1} | h_K.$$

- (b) Si K es imaginario, $d < 0$, $\varepsilon = 1$, $\chi(-1) = -1$. Por lo tanto $\chi(-1) = (-1)^\varepsilon = -1 = \chi_2(-1) \prod_{j=1}^t \chi_{q_j}(-1) = (-1)^{1+t}$. Por lo tanto t es par y

$$L = \mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \dots, \sqrt{p_s}, \sqrt{-q_1}, \dots, \sqrt{-q_t}) \quad \text{y} \quad 2^{s+t} | h_K.$$

Resumiendo, si K es real $2^{m-2} | h_K$ donde m es el número de primos que dividen a d y $2^{m-1} | h_K$ en el caso en que K es imaginario.

Los Ejemplos 6.4.7, 6.4.8, 6.4.9 y 6.4.10 son casos particulares de lo que se conoce como *campos de géneros*. El concepto de campo de géneros se remonta a Gauss [17] en el contexto de formas cuadráticas binarias. Para cualquier extensión finita K/\mathbb{Q} , el campo de géneros se define como la máxima extensión K_g no ramificada de K tal que K_g es la composición de K y de una extensión abeliana k^* de \mathbb{Q} : $K_g = Kk^*$. Esta definición se debe a Frölich [16]. Si K_H denota el campo de clase de Hilbert de K (Teorema 1.4.3), se tiene $K \subseteq K_g \subseteq K_H$. Originalmente la definición de campos de géneros fue dada para una extensión cuadrática de \mathbb{Q} . De hecho Gauss probó que si t es el número de primos positivos diferentes que dividen al discriminante δ_K de un campo cuadrático numérico K , entonces el 2-rango del grupo de clases de K es 2^{t-2} si $\delta_K > 0$ y existe un primo $p \equiv 3 \pmod{4}$ que divide a δ_K y 2^{t-1} en cualquier otro caso (ver Ejemplos 6.4.10 y 6.4.11).

H. Leopoldt [45] (ver Teorema 6.4.2) determinó el campo de géneros K_g de una extensión abeliana K de \mathbb{Q} usando caracteres de Dirichlet, generalizando de esta manera el trabajo de H. Hasse [21] el cual introdujo la teoría del género para campos cuadráticos numéricos.

M. Ishida determinó el campo de géneros K_g de cualquier extensión abeliana finita de \mathbb{Q} [31]. X. Zhang [79] dio una expresión simple de K_g para cualquier extensión abeliana K de \mathbb{Q} usando la teoría de ramificación de Hilbert.

En esta subsección presentamos brevemente la teoría del género.

Sea K un campo numérico, es decir, una extensión finita de \mathbb{Q} . Sea K_H el campo de clase de Hilbert de K , esto es, K_H es la máxima extensión abeliana no ramificada de K . Entonces el campo de géneros K_g de K es la máxima extensión de K contenida en K_H tal que sea la composición de K y de una extensión abeliana k^* de \mathbb{Q} . Equivalentemente, $K_g = Kk^* \subseteq K_H$ con k^* siendo la máxima extensión abeliana de \mathbb{Q} contenida en K_H .

A continuación presentamos la teoría del género en el caso abeliano para campos numéricos [45]. La teoría que presentamos está basada en el Teorema

6.4.2. En este caso K_g es la máxima extensión de K contenida en K_H tal que K_g/\mathbb{Q} es abeliana. Así pues, en esta sección consideramos K/\mathbb{Q} una extensión abeliana. Por el Teorema de Kronecker–Weber (Teorema 4.2.7) existe $n \in \mathbb{N}$ tal que $K \subseteq \mathbb{Q}(\zeta_n)$, donde ζ_n denota una raíz n -ésima primitiva de uno. Sea X el grupo de caracteres de Dirichlet asociado a K .

El siguiente ejemplo es un teorema debido a Gauss. No es más que el Ejemplo 6.4.10 visto de manera más estructural.

Ejemplo 6.4.11 (Teorema del Género de Gauss). Sea $K = \mathbb{Q}(\sqrt{d})$ una extensión cuadrática de \mathbb{Q} , donde $d \in \mathbb{Z}$ es libre de cuadrados. Sea m el número de factores primos diferentes de δ_K , el discriminante de K . Si p_1, \dots, p_m son estos factores, seleccionamos, $p_1 = 2$ si $2 \mid \delta_K$.

Sea χ el caracter cuadrático asociado a K . Entonces $\chi_{p_i} \neq 1$, $1 \leq i \leq m$ y $\chi_q = 1$ para todo $q \in \mathcal{P} \setminus \{p_1, \dots, p_m\}$. Para $p_i \neq 2$, χ_{p_i} es único y $\chi_{p_i}(-1) = (-1)^{(p_i-1)/2}$. En este caso el campo asociado a χ_{p_i} es $\mathbb{Q}(\sqrt{(-1)^{(p_i-1)/2}p_i})$. Si $p_1 = 2$, entonces hay tres caracteres cuadráticos $\chi_{p_1} = \chi_2$; dos de ellos tienen conductor 8, uno es real y el otro imaginario, y el otro tiene conductor 4. Si χ_2 es real, $\chi(-1) = 1$ y el campo asociado es $\mathbb{Q}(\sqrt{2})$. Si χ_2 es imaginario de conductor 8, $\chi(-1) = -1$ y el campo asociado es $\mathbb{Q}(\sqrt{-2})$. Finalmente, si χ_2 es de conductor 4, $\chi(-1) = -1$ y el campo asociado a χ_2 es $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Se sigue que la máxima extensión abeliana de \mathbb{Q} no ramificada en ningún primo finito es $J = \mathbb{Q}(\sqrt{\varepsilon}, \sqrt{(-1)^{(p_i-1)/2}p_i} \mid 2 \leq i \leq m)$ donde $\varepsilon = (-1)^{(p_1-1)/2}p_1$ si $p_1 \neq 2$ y $\varepsilon = 2, -2$ o -1 si $p_1 = 2$.

Obtenemos que $[J : \mathbb{Q}] = 2^m$ y que $[J : K] = 2^{m-1}$. Se tiene que $K_g = J$ excepto cuando K es real y J es imaginario y este último caso ocurre cuando $\delta_K > 0$ ($d > 0$) y existe $p_i \equiv 3 \pmod{4}$. En este caso, $[J^+ : K] = 2^{m-2}$. Por ejemplo, para la extensión cuadrática $K = \mathbb{Q}(\sqrt{-14})$ sobre \mathbb{Q} , tenemos $K_g = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ y para $K = \mathbb{Q}(\sqrt{79})$ obtenemos $J = \mathbb{Q}(\sqrt{-79}, i)$ y $K_g = J^+ = J \cap \mathbb{R} = \mathbb{Q}(\sqrt{79}) = K$.

Ahora si \mathcal{C}_K es el grupo de clase de K , $\mathcal{C}_K \cong \text{Gal}(K_H/K)$ y E es el campo fijo de \mathcal{C}_K^2 , entonces $\text{Gal}(E/K) \cong \mathcal{C}_K/\mathcal{C}_K^2$. Puesto que K_g es la máxima extensión abeliana de \mathbb{Q} contenida en K_H , K_g es el subcampo fijado de K_H bajo el grupo derivado G' de G . Puede ser verificado que (ver [38]) $G' = \mathcal{C}_K^2$ así que $K_g = E$ y se sigue que el 2-rango de \mathcal{C}_K es 2^{m-1} a menos que $d > 0$ y existe un primo $p \equiv 3 \pmod{4}$ que divide a d y en este caso el 2-rango de \mathcal{C}_K es 2^{m-2} .

Ejemplo 6.4.12. Si p es un primo impar, K es una extensión cíclica de \mathbb{Q} de grado p y si m es el número de primos ramificados en K , se sigue que K_g es una p -extensión elemental abeliana de \mathbb{Q} de grado p^m y $[K_g : K] = p^{m-1}$. En particular $p^{m-1} \mid |\mathcal{C}_K|$.

Ahora sea K una extensión abeliana de \mathbb{Q} con grupo de caracteres de Dirichlet X . Consideremos para cada $p \in \mathcal{P}$, X_p . Sea J el campo asociado a $\prod_{p \in \mathcal{P}} X_p$. Sea $p^{m_p} := \text{mcm}\{\mathfrak{f}_{\chi_p} \mid \chi \in X\}$ donde \mathfrak{f}_{χ_p} denota al conductor de χ_p . Entonces el campo K_p asociado a X_p está contenido en $\mathbb{Q}(\zeta_{p^{m_p}})$ pero no en

$\mathbb{Q}(\zeta_{p^{m_p-1}})$. Si p es impar, K_p es el único subcampo de $\mathbb{Q}(\zeta_{p^{m_p}})$ de grado $|X_p|$ sobre \mathbb{Q} y K_p/\mathbb{Q} es una extensión cíclica. Si $p = 2$, K_2 es uno de los siguientes campos. Si $|X_2| = \varphi(2^{m_2}) = 2^{m_2-1}$, $K_2 = \mathbb{Q}(\zeta_{2^{m_2}})$. Si $|X_2| = \frac{\varphi(2^{m_2})}{2} = 2^{m_2-2}$, $K_2 = \mathbb{Q}(\zeta_{2^{m_2}})^+ = \mathbb{Q}(\zeta_{2^{m_2}} + \zeta_{2^{m_2}}^{-1}) = \mathbb{Q}(\zeta_{2^{m_2}}) \cap \mathbb{R}$ si $\chi(-1) = 1$ para todo $\chi \in X$ y $K_2 = \mathbb{Q}(\zeta_{2^{m_2}} - \zeta_{2^{m_2}}^{-1})$ si existe $\chi \in X$ con $\chi(-1) = -1$.

Por lo tanto, si K y J son ambos reales o ambos imaginarios, $K_g = J = \prod_{p \in \mathcal{P}} K_p$. Si K es real y J es imaginario, $K_g = J^+ = J \cap \mathbb{R}$.

6.4.2. Grupos abelianos como grupos de Galois y de clases

Sea G un grupo abeliano finito dado. Escribamos $G = C_{n_1} \times \cdots \times C_{n_r}$. El primer resultado es que G es realizable como grupo de Galois sobre cualquier campo numérico.

Teorema 6.4.13. *Sea E cualquier campo numérico y sea G un grupo abeliano finito arbitrario. Entonces existen una infinidad de campos F tales que F/E es una extensión de Galois y tales que $G \cong \text{Gal}(F/E)$.*

Demostración. Sean q_1, \dots, q_s los primos ramificados en E/\mathbb{Q} . Puesto que hay una infinidad de primos congruentes a 1 módulo n con $n \in \mathbb{N}$ dado (Corolario 5.1.3), seleccionamos primos p_1, \dots, p_r tales que $p_1 < p_2 < \cdots < p_r$, $q_1, \dots, q_s < p_1$ y $p_i \equiv 1 \pmod{n_i}$, $1 \leq i \leq r$.

Para cada $1 \leq i \leq r$, sea M_i el único subcampo de $\mathbb{Q}(\zeta_{p_i})$ tal que $[M_i : \mathbb{Q}] = n_i$ el cual existe pues $n_i | p_i - 1 = [\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}]$. Se tiene que M_i/\mathbb{Q} es cíclica de grado n_i y p_i es el único primo finito ramificado en M_i/\mathbb{Q} . Puesto que los primos ramificados en cada M_i son distintos entre sí y distintos a los primos ramificados en E/\mathbb{Q} , se tiene que si $M := M_1 \cdots M_r$, entonces $\text{Gal}(M/\mathbb{Q}) \cong \prod_{i=1}^r \text{Gal}(M_i/\mathbb{Q}) \cong \prod_{i=1}^r C_{n_i} \cong G$ y $M \cap E = \mathbb{Q}$. Sea $F := ME$. Por Teoría de Galois tenemos que F/E es una extensión de Galois y $\text{Gal}(F/E) \cong \text{Gal}(M/M \cap E) = \text{Gal}(M/\mathbb{Q}) \cong G$.

Puesto que tenemos una infinidad de selecciones para los números primos p_1, \dots, p_r , hay una infinidad de campos M no isomorfos que satisfacen lo anterior. \square

Podemos mejorar en ciertos aspectos el Teorema 6.4.13.

Teorema 6.4.14. *Sea G un grupo abeliano finito. Entonces existen campos numéricos L y K tales que:*

- (a) $\text{Gal}(L/K) \cong G$,
- (b) L/K es no ramificada en ningún primo, incluyendo a los primos infinitos.
- (c) Se puede seleccionar L/\mathbb{Q} una extensión abeliana y K/\mathbb{Q} una extensión cíclica.

Demostración. Sea $G \cong C_{n_1} \times \cdots \times C_{n_r}$. Nuevamente seleccionamos primos distintos p_1, \dots, p_r tales que $p_i \equiv 1 \pmod{2n_i}$, $1 \leq i \leq r$ (el papel que juega el 2 en estas congruencias será relacionado más adelante con el comportamiento de los primos infinitos en las extensiones).

Se tiene que $\text{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}) \cong U_{p_i} \cong C_{p_i-1}$. Sea ψ_i un caracter de conductor p_i que genere al grupo cíclico $\widehat{U_{p_i}}$, es decir, ψ_i es de orden $p_i - 1$. Consideremos el caracter $\chi_i := \psi_i^{(p_i-1)/n_i}$. Puesto que $2 \mid \frac{p_i-1}{n_i}$ se sigue que $\chi_i(-1) = 1$ para toda $1 \leq i \leq r$.

Sea p_{r+1} un primo impar distinto a p_1, \dots, p_r y tal que $p_{r+1} \equiv 1 \pmod{n_1 \cdots n_r}$. Ahora sea χ_{r+1} cualquier caracter de conductor p_{r+1} y tal que $\chi_{r+1}(-1) = -1$ y tal que $n_1 \cdots n_r \mid o(\chi_{r+1})$. Tal caracter existe, por ejemplo, podemos tomar χ_{r+1} un generador de $\widehat{U_{p_{r+1}}}$. La condición $\chi_{r+1}(-1) = -1$ la usaremos para construir K imaginario.

Sea $\chi := \chi_1 \chi_2 \cdots \chi_r \chi_{r+1}$. Sea K el campo asociado a χ , o más precisamente, al grupo $X = \langle \chi \rangle$. Se sigue que K/\mathbb{Q} es una extensión cíclica pues $\text{Gal}(K/\mathbb{Q}) \cong \widehat{\langle \chi \rangle} \cong \langle \chi \rangle$.

Ahora bien, $\chi(-1) = \chi_1(-1) \cdots \chi_r(-1) \chi_{r+1}(-1) = -1$ lo cual implica que K es imaginario y en particular toda extensión de K es no ramificada en los primos infinitos.

Sea $Y := \langle \chi_1, \dots, \chi_r, \chi_{r+1} \rangle$ y sea L el campo asociado a Y . Entonces L/\mathbb{Q} es una extensión abeliana y se sigue que L y K satisfacen (c).

Puesto que $f_{\chi_i} = p_i$ se sigue que $Y_{p_i} = X_{p_i} = \langle \chi_i \rangle$, $1 \leq i \leq r+1$ y $Y_p = X_p = \{1\}$ para todo primo $p \neq p_1, \dots, p_r, p_{r+1}$. Se sigue del Teorema 6.3.3 que L/K es no ramificada en ningún primo pues

$$e_{p_i}(L/\mathbb{Q}) = |Y_{p_i}| = |\langle \chi_{p_i} \rangle|, \quad e_{p_i}(K/\mathbb{Q}) = |X_{p_i}| = |\langle \chi \rangle_{p_i}| = |\langle \chi_{p_i} \rangle|,$$

$1 \leq i \leq r+1$.

Ahora bien, puesto que $\chi = \chi_1 \cdots \chi_r \chi_{r+1}$, $\chi_{r+1} = \chi_1^{-1} \cdots \chi_r^{-1} \chi$ y por lo tanto

$$Y = \langle \chi_1, \dots, \chi_r, \chi_{r+1} \rangle = \langle \chi_1, \dots, \chi_r, \chi \rangle \quad (6.7)$$

de donde se obtiene

$$\text{Gal}(L/K) \cong \widehat{\text{Gal}(L/K)} \cong \frac{\widehat{\text{Gal}(L/\mathbb{Q})}}{\text{Gal}(L/K)^\perp} \cong \frac{Y}{X} = \frac{Y}{\langle \chi \rangle}. \quad (6.8)$$

Consideremos ahora los mapeos naturales

$$\langle \chi_1, \dots, \chi_r \rangle \xrightarrow{i} X \xrightarrow{\pi} Y/\langle \chi \rangle$$

y sea $\varphi = \pi \circ i$ y de (6.7) se sigue que φ es suprayectiva.

Sea ahora $\chi_1^{\alpha_1} \cdots \chi_r^{\alpha_r} \in \text{nuc } \varphi$, esto es, existe α tal que $\chi_1^{\alpha_1} \cdots \chi_r^{\alpha_r} = \chi^\alpha = \chi_1^\alpha \cdots \chi_r^\alpha \chi_{r+1}^\alpha$. Puesto que todos los caracteres tienen conductores primos relativos a pares, se sigue que $\chi_{r+1}^\alpha = 1$ y que $\alpha_i \equiv \alpha \pmod{n_i}$, $n_i = o(\chi_i)$, para $1 \leq i \leq r$.

Puesto que $n_1 \cdots n_r | o(\chi_{r+1})$, se tiene que $\alpha \equiv 0 \pmod{n_i}$ para $1 \leq i \leq r$ y por tanto $\alpha_i \equiv 0 \pmod{n_i}$ para toda i . Se sigue que $\chi_1^{\alpha_1} \cdots \chi_r^{\alpha_r} = 1$ y que núc $\varphi = \{1\}$, es decir φ es un isomorfismo entre $\langle \chi_1, \dots, \chi_r \rangle$ y $Y/\langle \chi \rangle$. Por tanto, de (6.8) se sigue que

$$\begin{aligned} \text{Gal}(L/\mathbb{Q}) &\cong \frac{Y}{\langle \chi \rangle} \cong \langle \chi_1, \dots, \chi_r \rangle \cong \bigoplus_{i=1}^r \langle \chi_i \rangle \cong \\ &\cong \bigoplus_{i=1}^r \langle \psi_i^{(p_i-1)/n_i} \rangle \cong \bigoplus_{i=1}^r C_{n_i} \cong G. \end{aligned} \quad \square$$

Como corolarios al Teorema 6.4.14 y al Teorema de clase de Hilbert, podemos enunciar:

Corolario 6.4.15. *Sea G un grupo abeliano finito. Entonces existe una extensión cíclica del campo de los números racionales K/\mathbb{Q} tal que el grupo de clases de ideales de K contiene un subgrupo isomorfo a G . En otras palabras, $G \subseteq C_K$.*

Demostración.

Sea H_K el campo de clase de Hilbert de K , esto es, $\text{Gal}(H_K/K) \cong C_K$ y H_K es la máxima extensión abeliana de K no ramificada en ningún primo incluyendo a los primos infinitos. Sea L/K como en el Teorema 6.4.14. Entonces $L \subseteq H_K$ y si $H := \text{Gal}(H_K/L)$, entonces $\text{Gal}(L/K) \cong C_K/H \cong G$. Así, C_K tiene un grupo cociente isomorfo a G . Por la Proposición 6.1.15 se sigue que C_K tiene un subgrupo isomorfo a G . \square

Proposición 6.4.16. *Sea L/K una extensión de campos numéricos tal que no existe ninguna subextensión E/K con $E \subseteq L$, E/K no ramificada en ningún primo incluyendo a los primos infinitos y tal que $\text{Gal}(E/K)$ es un grupo abeliano. Entonces $h_K | h_L$, donde en general h_* denota al número de clase del campo $*$.*

Demostración.

Sea H_K la máxima extensión abeliana de K no ramificada. Entonces $L \subseteq LH_K \subseteq H_L$. $\text{Gal}(H_K/K) \cong C_K$. Ahora, por hipótesis se sigue que $H_K \cap L = K$ pues $H_K \cap L$ es una extensión abeliana de K no ramificada y contenida en L . En particular $[LH_K : L] = [H_K : K]$. Ahora bien LH_K es una extensión abeliana de L no ramificada por lo que $LH_K \subseteq H_L$. En particular

$$[LH_K : L] = [H_K : K] = |C_K| = h_K | h_L = [H_L : L]. \quad \square$$

Definición 6.4.17. Un campo numérico K , se llama *totalmente real* si todos sus encajes en \mathbb{C} caen en \mathbb{R} . Ahora K se llama *totalmente imaginario* si ninguno de sus encajes está contenido en \mathbb{R} .

Un campo K se llama de tipo MC (MC significa *multiplicación compleja*) si es un campo totalmente imaginario que es una extensión cuadrática de un campo totalmente real K^+ .

Ejemplo 6.4.18. Para $n \geq 3$, $\mathbb{Q}(\zeta_n)$ es un campo de tipo MC con $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Corolario 6.4.19. Si K es un campo de tipo MC entonces $h_{K^+} | h_K$. En particular $h_{\mathbb{Q}(\zeta_n)^+} | h_{\mathbb{Q}(\zeta_n)}$.

Demostración. La extensión K/K^+ satisface las hipótesis de la Proposición 6.4.16 pues K/K^+ es ramificada en los primos infinitos. \square

Series L de Dirichlet

7.1. Teorema de Dirichlet

En esta sección nos proponemos probar que si $a, b \in \mathbb{Z}$ son primos relativos, entonces existen una infinidad de primos de la forma $a + nb$ con $n \in \mathbb{N}$.

Claramente la condición de que a y b sean primos relativos es necesaria pues si existe $d > 1$ tal que $d|a$ y $d|b$ entonces $d|a + nb$ y en este caso a lo más podría haber un primo de la forma $a + nb$, a saber, d .

El Corolario 5.1.3 nos provee de una demostración elemental para el caso $a = 1$ y $b = n \in \mathbb{N}$ arbitrario. E. Landau [41] da una demostración elemental para el caso $a = -1$ y $b = n$ arbitrario. Mediante técnicas completamente elementales, se pueden probar numerosos casos particulares del Teorema de Dirichlet: primos de la forma $3n + 1, 3n + 2, 4n + 1, 4n + 3, 8n + 1, 8n + 3, 8n + 5, 8n + 7, 6n + 5$, etc. El caso $1 + tn$ tiene muchas demostraciones elementales, algunas más elementales que la que dimos en el Corolario 5.1.3. En el Teorema 7.1.1 indicamos otra demostración, mucho más básica que la del Corolario 5.1.3 pero no daremos todos los detalles.

Teorema 7.1.1. *Sea $n \in \mathbb{N}$ cualquiera. Entonces hay una infinidad de primos de la forma $p \equiv 1 \pmod{n}$.*

Demostración. Sea S un conjunto y sea $f: S \rightarrow S$ una función. Sea $T_n := \{s \in S \mid f^{(n)}(s) = s\}$, $n \in \mathbb{N}$. Para $s \in T_n$ sea d el mínimo número natural tal que $f^{(d)}(s) = s$. Entonces $d \leq n$. Escribamos $n = qd + r$ con $0 \leq r \leq d - 1$. Entonces $f^{(r)}(s) = s$. Puesto que $r \leq d - 1$ se sigue que $r = 0$ y $d|n$.

Definimos el conjunto $P_d := \{s \in T_n \mid o(s) = d\}$ y para $s \in P_n$, se tiene que $f^{(0)}(s), \dots, f^{(n-1)}(s)$ son todos distintos y en particular $n \mid |P_n|$.

Además $T_n = \cup_{d|n} P_d$ y $P_{d_1} \cap P_{d_2} = \emptyset$ para $d_1 \neq d_2$. Se sigue que $|T_n| = \sum_{d|n} |P_d|$. Por la fórmula de inversión de Möbius, obtenemos que

$$|P_n| = \sum_{d|n} \mu\left(\frac{n}{d}\right) |T_d|, \text{ donde } \mu(m) = \begin{cases} 1 & \text{si } m = 1 \\ (-1)^r & \text{si } m = p_1 \cdots p_r. \\ 0 & \text{en otro caso} \end{cases}$$

En particular $n | \sum_{d|n} \mu\left(\frac{n}{d}\right) |T_d|$.

Sean a y n enteros mayores que uno y sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la descomposición de n en primos. Sea q un divisor común de

$$\frac{a^n - 1}{a^{n/p_1} - 1}, \dots, \frac{a^n - 1}{a^{n/p_r} - 1}.$$

Para cualesquiera enteros $\alpha_0, \dots, \alpha_{n-1}$ con $0 \leq \alpha_i \leq a-1$, $1 \leq i \leq n$ definimos

$$(\alpha_0, \dots, \alpha_{n-1})_a := \sum_{i=0}^{n-1} \alpha_i a^i = \alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1} a^{n-1}.$$

Sea $S := \{\alpha = (\alpha_0, \dots, \alpha_{n-1})_a \mid q \nmid \alpha\}$. Si $q = 1$ entonces $S = \emptyset$. Definimos la función $f: S \rightarrow S$ dada por

$$f(\alpha) = (\alpha_{n-1}, \alpha_0, \dots, \alpha_{n-2})_a = \alpha_{n-1} + \alpha_0 a + \cdots + \alpha_{n-2} a^{n-1}.$$

Entonces obtenemos $T_n = S$, y por tanto

$$|T_n| = |S| = a^n - 1 - \frac{a^n - 1}{q} = \frac{(a^n - 1)(q - 1)}{q}$$

lo cual implica que $n | \frac{(a^n - 1)(q - 1)}{q}$.

Si $n = 1$ no hay nada que probar. Supongamos $n > 1$ y sean $\{q_1, \dots, q_s\}$ primos de la forma $1 + nt$. Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Consideremos los polinomios

$$f_1(x) = \frac{x^n - 1}{x^{n/p_1} - 1}, \dots, f_r(x) = \frac{x^n - 1}{x^{n/p_r} - 1}.$$

Todos estos polinomios tienen como raíz común a ζ_n por lo que existe un polinomio $g(x)$ no constante con coeficientes enteros y coeficiente líder 1 tal que $g(x)$ divide a $f_i(x)$ para $i = 1, 2, \dots, r$.

Se tiene que $f_i(0) = 1$ lo cual implica que $g(0) = \pm 1$. En particular, si a es cualquier entero, entonces $g(a) \equiv \pm 1 \pmod{a}$, esto es, a y $g(a)$ son primos relativos. Además $\lim_{x \rightarrow \infty} g(x) = \infty$. Sea $t_0 \in \mathbb{N}$ con $g(a) > 1$ para todo $a > t_0$. Definimos $a := nt_0 q_1 \cdots q_s$. Si $s = 0$, entonces $a := nt_0$. Si q es cualquier número primo que divide a $g(a) > 1$ entonces $q \nmid a$ por lo que $q \neq q_i$ para toda $i = 1, \dots, s$ y puesto que $n | (a^n - 1)(q - 1)$ y $n | a$, se tiene que n y $a^n - 1$ son primos relativos lo cual implica que $n | q - 1$, es decir $q \equiv 1 \pmod{n}$ y este es un nuevo primo de la forma $1 + nt$. \square

Ya que hemos mencionado que algunos casos particulares del Teorema de Dirichlet tienen demostraciones elementales, resulta que no existe, hasta ahora, una demostración elemental del caso general. En esta sección presentaremos la demostración del caso general.

Definición 7.1.2. Sea $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ un caracter de Dirichlet módulo k , es decir, entendemos $\chi(a) = 0$ si $\text{mcd}(a, k) > 1$. Se define la *L-serie de Dirichlet* por

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

A grandes rasgos, la demostración del Teorema de Dirichlet es como sigue. Sean $\text{mcd}(a, b) = 1$ y consideremos todos los caracteres de Dirichlet módulo a . Entonces la serie $L(s, \chi)$ es una función analítica para $s > 1$ y se tiene

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

donde el producto es sobre todos los números primos.

Tomando logaritmos y derivando, se obtiene

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_p \frac{\chi(p) \ln p}{p^s - \chi(p)}.$$

Sea $\Lambda: \mathbb{N} \rightarrow \mathbb{C}$ dada por $\Lambda(n) = \begin{cases} \ln p & \text{si } n = p^c, c \geq 1 \\ 0 & \text{en otro caso} \end{cases}$. Entonces

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s}.$$

Definición 7.1.3. La función $\Lambda(n)$ se llama la *función de von-Mangoldt*.

Ahora bien, multiplicando por $\overline{\chi(b)}$ y sumando sobre todos los caracteres μ se obtiene

$$\sum_{n \equiv b \pmod{a}} \frac{\Lambda(n)}{n^s} = \frac{1}{\varphi(a)} \sum_{\mu} \overline{\mu(b)} \frac{-L'(s, \mu)}{L(s, \mu)}.$$

Ahora cuando $s \rightarrow 1^+$ el lado izquierdo es aproximadamente $\sum_{p \equiv b \pmod{a}} \frac{\ln p}{p}$ y el lado derecho se va a infinito lo cual prueba lo que queremos.

Ahora bien, si $\chi = 1$, se puede probar que $\lim_{s \rightarrow 1^+} -\frac{L'(s, \chi_0)}{L(s, \chi_0)} = \infty$. Por tanto, para ver que el lado derecho se va infinito basta probar que $\frac{L'(s, \chi)}{L(s, \chi)}$ permanece acotado cuando $s \rightarrow 1^+$ y $\chi \neq 1$, es decir, el problema central es ver que $L(1, \chi) \neq 0$ para $\chi \neq 1$. A continuación presentamos este desarrollo.

Teorema 7.1.4. Para todo caracter de Dirichlet χ módulo k , $L(s, \chi)$ es analítica para $s \in \mathbb{C}$, $\text{Re } s > 1$. Además, para esta región, $L(s, \chi)$ tiene una representación como producto de Euler

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Demostración. Se tiene $|\chi(n)| \leq 1$ por lo que $|\frac{\chi(n)}{n^s}| \leq \frac{1}{|n^s|} = \frac{1}{n^x}$ donde $x = \operatorname{Re} s$ lo cual converge para $x > 1$. Por tanto $L(s, \chi)$ es absolutamente convergente para $x > 1$.

Ahora para $\varepsilon > 0$ y $x \geq 1 + \varepsilon$, $(\sum_{n=1}^m \frac{\chi(n)}{n^s})' = -\sum_{n=1}^m \frac{\chi(n) \ln n}{n^s}$ y $|\sum_{n=1}^m \frac{\chi(n) \ln n}{n^s}| \leq \sum_{n=1}^m \frac{\ln n}{n^{1+\varepsilon}}$ la cual converge.

Por el criterio M de Weierstrass se tiene que $-\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s}$ converge absoluta y uniformemente para $x \geq 1 + \varepsilon$, $\varepsilon > 0$. Puesto que $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converge absoluta y uniformemente para $x \geq 1 + \varepsilon$, se sigue que se puede diferenciar término a término y

$$L'(s, \chi) = -\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s} \quad \text{para } x > 1.$$

Ahora, por la misma razón que antes, $\sum_{n=1}^{\infty} \frac{\mu(n)\chi(n)}{n^s}$ converge absolutamente para $x > 1$ y uniformemente para $x \geq 1 + \varepsilon$, $\varepsilon > 0$. Aquí, $\mu(n)$ es la función mu de Moebius.

Se tiene que μ satisface $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$ (Lema 3.2.14). Por tanto

$$\begin{aligned} \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\mu(n)}{n^s} &= \sum_{t=1}^{\infty} \sum_{mn=t} \frac{\chi(m)\chi(n)\mu(n)}{m^s n^s} \\ &= \sum_{t=1}^{\infty} \frac{\chi(t)}{t^s} \sum_{n|t} \mu(n) = \frac{\chi(1)}{1^s} = 1 \end{aligned}$$

es decir,

$$L(s, \chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\mu(n)}{n^s} = 1 \quad (7.1)$$

y en particular $L(x, \chi) \neq 0$ para $x := \operatorname{Re} s > 1$.

Finalmente, para $m > 1$, sea S el conjunto de los números naturales n no divisibles por ningún primo $p > m$. Entonces si p_1, \dots, p_r son todos los primos menores o iguales a m :

$$\prod_{p \leq m} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{i=1}^r \left(1 - \frac{\chi(p_i)}{p_i^s}\right) = \sum_{\substack{1 \leq i_1 < i_2 < \dots < i_t \leq r \\ 0 \leq t \leq r}} \frac{(-1)^t \chi(p_{i_1} \cdots p_{i_t})}{(p_{i_1} \cdots p_{i_t})^s}$$

y

$$\begin{aligned}
\sum_{n \in S} \frac{\chi(n)\mu(n)}{n^s} &= \sum_{\alpha_1=0}^{\infty} \cdots \sum_{\alpha_r=0}^{\infty} \frac{\chi(p_1^{\alpha_1} \cdots p_r^{\alpha_r})\mu(p_1^{\alpha_1} \cdots p_r^{\alpha_r})}{(p_1^{\alpha_1} \cdots p_r^{\alpha_r})^s} \\
&= \sum_{\substack{1 \leq i_1 < i_2 < \cdots < i_t \leq r \\ 0 \leq t \leq r}} \frac{\chi(p_{i_1} \cdots p_{i_t})}{(p_1^{\alpha_1} \cdots p_r^{\alpha_r})^s} \mu(p_{i_1} \cdots p_{i_t}) \\
&= \sum_{\substack{1 \leq i_1 < i_2 < \cdots < i_t \leq r \\ 0 \leq t \leq r}} \frac{(-1)^t \chi(p_{i_1} \cdots p_{i_t})}{(p_{i_1} \cdots p_{i_t})^s}.
\end{aligned}$$

Es decir

$$\prod_{p \leq m} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n \in S} \frac{\chi(n)\mu(n)}{n^s} = \sum_{n=1}^m \frac{\chi(n)\mu(n)}{n^s} + \sum_{\substack{n' \in S \\ n' > m}} \frac{\chi(n')\mu(n')}{(n')^s}.$$

Por (7.1) se sigue que $\lim_{m \rightarrow \infty} \sum_{n=1}^m \frac{\chi(n)\mu(n)}{n^s} = L(s, \chi)^{-1}$, $\operatorname{Re} s > 1$. Ahora

$$\sum_{\substack{n' \in S \\ n' > m}} \left| \frac{\chi(n')\mu(n')}{(n')^s} \right| \leq \sum_{n=m+1}^{\infty} \frac{1}{n^s} \xrightarrow{m \rightarrow \infty} 0 \quad \text{para } \operatorname{Re} s > 1.$$

Por tanto $\prod_p \left(1 - \frac{\chi(p)}{p^s}\right) = \frac{1}{L(s, \chi)}$ y

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \quad \operatorname{Re} s > 1. \quad \square$$

Definición 7.1.5. Sea K un campo numérico, $[K : \mathbb{Q}] < \infty$. La *función zeta de Dedekind* de K se define por

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}$$

donde \mathfrak{a} recorre los ideales no cero de \mathcal{O}_K y $N\mathfrak{a} := |\mathcal{O}_K/\mathfrak{a}|$.

En particular si $K = \mathbb{Q}$, obtenemos la *función zeta de Riemann*:

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Como en el Teorema 7.1.4 obtenemos

Teorema 7.1.6. Se tiene que $\zeta_K(s)$ converge absolutamente para $\operatorname{Re} s > 1$, uniformemente para $\operatorname{Re} s \geq 1 + \varepsilon$, $\varepsilon > 0$ y se tiene

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}, \quad \operatorname{Re} s > 1$$

donde \mathfrak{p} recorre todos los ideales primos no cero de \mathcal{O}_K . \square

Proposición 7.1.7.

(a) Para $\Re s > 1$ tenemos

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}$$

donde $\Lambda(n)$ es la función de von-Mangoldt.

(b) Si $\chi_0 = 1$ módulo k , es decir, $\chi(n) = 1$ si $\text{mcd}(n, k) = 1$ y $\chi_0(n) = 0$ en otro caso, entonces

$$\lim_{s \rightarrow 1} \left| \frac{L'(s, \chi_0)}{L(s, \chi_0)} \right| = \infty \quad y \quad \lim_{\substack{s \in \mathbb{R} \\ s \rightarrow 1^+}} \frac{L'(s, \chi_0)}{L(s, \chi_0)} = -\infty.$$

Demostración. Se tiene que $\left| \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{\ln n}{n^x} < \infty$ para $x = \Re s > 1$.

Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^r \sum_{\beta_i=0}^{\alpha_i} \Lambda(p_i^{\beta_i}) = \sum_{i=1}^r \sum_{\beta_i=1}^{\alpha_i} \ln p_i = \sum_{i=1}^r \ln p_i^{\alpha_i} = \ln n.$$

Para $\Re s = x > 1$, se tiene:

$$\begin{aligned} L(s, \chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} &= \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} \\ &= \sum_{t=1}^{\infty} \frac{1}{t^s} \left(\sum_{mn=t} \chi(mn)\Lambda(n) \right) = \sum_{t=1}^{\infty} \frac{\chi(t)}{t^s} \left(\sum_{n|t} \Lambda(n) \right) \\ &= \sum_{t=1}^{\infty} \frac{\chi(t) \ln t}{t^s} = -L'(s, \chi) \end{aligned}$$

de donde se obtiene (a).

Ahora bien, si $\chi_0 = 1$ módulo k , entonces

$$\begin{aligned}
\frac{L'(s, \chi_0)}{L(s, \chi_0)} &= - \sum_{n=1}^{\infty} \frac{\chi_0(n) \Lambda(n)}{n^s} = - \sum_{\substack{n=1 \\ \text{mcd}(n,k)=1}}^{\infty} \frac{\Lambda(n)}{n^s} \\
&= - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \sum_{\text{mcd}(n,k)>1} \frac{\Lambda(n)}{n^s} = - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \sum_{p|k} \sum_{m=1}^{\infty} \frac{\Lambda(p^m)}{(p^m)^s} \\
&= - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \sum_{p|k} \sum_{m=1}^{\infty} \frac{\ln p}{(p^m)^s} \\
&= - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \sum_{p|k} \ln p \left(\frac{1}{1-p^s} - 1 \right) \\
&= - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \sum_{p|k} \frac{p^s \ln p}{1-p^s}.
\end{aligned}$$

Como $\{p \mid p|k\}$ es un conjunto finito y $\lim_{s \rightarrow 1} \frac{p^s \ln p}{1-p^s} = \frac{p \ln p}{1-p} < \infty$, para ver que $\lim_{s \rightarrow 1} \left| \frac{L'(s, \chi_0)}{L(s, \chi_0)} \right| = \infty$ basta ver que $\lim_{s \rightarrow 1} \left| \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \right| = \infty$.

Se tiene que $\sum_{p \text{ primo}} \frac{\ln p}{p} \geq \sum_{p \text{ primo}} \frac{1}{p}$. Ahora

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n} = \sum_{p \text{ primo}} \sum_{c=1}^{\infty} \frac{\Lambda(p^c)}{p^c} \geq \sum_{p \text{ primo}} \frac{\ln p}{p} \geq \sum_{p \text{ primo}} \frac{1}{p}.$$

Veamos que $\sum_{p \text{ primo}} \frac{1}{p} = \infty$. Sean p_1, \dots, p_r los primeros r primos. Se tiene $p_1 = 2 = 2^1 = 2^{2^0} = 2^{2^{1-1}}$, $p_2 = 3 < 4 = 2^2 = 2^{2^{2-1}}$. Supongamos que para $r > 1$, $p_r < 2^{2^{r-1}}$. Puesto que algún número primo p distinto de p_1, \dots, p_r divide a $p_1 \cdots p_r + 1$, se tiene que $p_{r+1} \leq p_1 \cdots p_r + 1 < 2 \cdot 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{r-1}} + 1 < 2^{2^r}$.

Si acaso $\sum_{p \text{ primo}} \frac{1}{p} = \sum_{i=1}^{\infty} \frac{1}{p_i}$ convergiese, existiría $n_0 \in \mathbb{N}$ tal que $\sum_{n=n_0+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$.

Para $x \in \mathbb{N}$ definamos $Q_{n_0}(x)$ el número de números naturales menores o iguales a x y que no son divisibles por ningún p_n con $n \geq n_0 + 1$. Ahora, dado p primo, el número de enteros positivos $m \leq x$ y divisibles por p es menor o igual a x/p . Por lo tanto

$$x - Q_{n_0} < \frac{x}{p_{n_0+1}} + \frac{x}{p_{n_0+2}} + \cdots \leq x \sum_{n=n_0+1}^{\infty} \frac{1}{p_n} < \frac{x}{2}.$$

Por lo tanto $x/2 < Q_{n_0}(x)$.

Sea $m < x$ y m no es divisible por ningún primo p_n con $n \geq n_0 + 1$. Escribamos $m = s^2 t$ donde t es libre de cuadrados, es decir, $t = 2^{a_1} 3^{a_2} \cdots p_{n_0}^{a_{n_0}}$

con $a_i \in \{0, 1\}$, esto es, t tiene a lo más 2^{n_0} selecciones y hay a lo más $\sqrt{m} < \sqrt{x}$ selecciones para s . Por lo tanto $\frac{x}{2} < Q_{n_0}(x) < 2^{n_0} \sqrt{x}$ pero esto es imposible pues $\lim_{x \rightarrow \infty} \frac{x/2}{2^{n_0} \sqrt{x}} = \infty$. Se sigue que $\sum_{p \text{ primo}} \frac{1}{p} = \infty$.

Entonces $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n}$ diverge. Dado $M \in \mathbb{R}$, $M > 0$, existe m tal que $\sum_{n=1}^m \frac{\Lambda(n)}{n} > M$. Se sigue que existe $\varepsilon = \varepsilon(M) > 0$ tal que para $1 < x < 1 + \varepsilon$, $\sum_{n=1}^m \frac{\Lambda(n)}{n^x} > M$, por tanto $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^x} > M$. De esto se sigue (b). \square

Damos tres resultados más antes de probar el Teorema de Dirichlet.

Lema 7.1.8. Si $n \geq m \geq 1$ y $x \neq 1$, entonces si φ es la función ϕ de Euler, se tiene

$$\left| \sum_{i=m}^t \chi(i) \right| < \frac{\varphi(k)}{2}.$$

Demostración. Puesto que $\chi \neq 1$, se tiene que $\sum_{\substack{a=1 \\ \text{mcd}(a,k)=1}}^k \chi(a) = 0$ donde χ está definido módulo k . Puesto que $\chi(a) = 0$ para $\text{mcd}(a, k) > 1$, se tiene que $\sum_{a=1}^k \chi(a) = 0$ y $\varphi(k)$ de estos términos satisfacen $|\chi(a)| = 1$ (estos son los que $\text{mcd}(a, k) = 1$).

Entonces si $n - m = tk + r$ con $0 \leq r \leq k - 1$, se tiene

$$\sum_{i=m}^n \chi(i) = \sum_{i=m}^{m+tk} \chi(i) + \sum_{i=m+tk+1}^{m+tk+r} \chi(i) = \sum_{i=m+tk+1}^{m+tk+r} \chi(i)$$

es decir, podemos suponer que $n - m \leq r \leq k - 1$.

Ahora bien, si en la suma $\sum_{i=m}^n \chi(i)$ hay a lo más $\varphi(k)/2$ términos con $|\chi(i)| = 1$, se tiene $\left| \sum_{i=m}^n \chi(i) \right| \leq \sum_{i=m}^n |\chi(i)| < \varphi(k)/2$.

Si en la suma hay más de $\varphi(k)/2$ términos con $|\chi(i)| = 1$, entonces puesto que $n \leq m + k - 1$, se tiene

$$\left| \sum_{i=m}^n \chi(i) \right| = \left| \sum_{i=m}^{m+k-1} \chi(i) - \sum_{n+1}^{m+k-1} \chi(i) \right| = \left| \sum_{i=n+1}^{m+k-1} \chi(i) \right| \leq \sum_{i=n+1}^{m+k-1} |\chi(i)| < \frac{\varphi(k)}{2}$$

pues en esta última suma hay menos de $\varphi(k)/2$ términos con $|\chi(i)| = 1$. \square

Lema 7.1.9. Si χ es cualquier caracter, $\chi_0 = 1$ y $s > 1$, entonces tenemos

$$|L(s, \chi_0)|^3 |L(s, \chi)|^4 |L(s, \chi^2)|^2 \geq 1 \quad (s \in \mathbb{R}).$$

Demostración. Si $x, y \in \mathbb{R}$ y $0 < x < 1$, se tiene

$$(1-x)^3 |1 - xe^{iy}|^4 |1 - xe^{2iy}|^2 < 1 \quad (7.2)$$

Para verificar (7.2), hagamos $a := \cos y$, $2a^2 - 1 = \cos 2y$. Entonces $|1 - xe^{iy}|^4 = (1 + x^2 - 2xa)^2$, $|1 - xe^{2iy}|^2 = (1 + x)^2 - 4xa^2$. Si definimos $\ell(a) = (1 + x^2 - 2xa)^2((1 + x)^2 - 4xa^2)$, $0 < x < 1$, $-1 \leq a \leq 1$, $\ell'(a_0) = 0$ para $|a_0| < 1 \iff a_0 = \frac{1+x^2}{2(1+x)^2}$ y $\ell''(a) > 0$ por lo que a_0 es un mínimo local para $\ell(a)$, $|a| \leq 1$. Ahora bien $\ell(-1) > \ell(a_0), \ell(1)$ por lo que el máximo en $-1 \leq a \leq 1$ es $\ell(-1) = (1+x)^4(1-x)^2$. Por lo tanto

$$(1-x)^3 |1 - xe^{iy}|^4 |1 - xe^{2iy}|^2 \leq (1-x)^3 (1+x)^4 (1-x)^2 = (1-x^2)^4 (1-x) < 1.$$

Ahora, si p es un número primo que no divide a k , tenemos $\chi(p) = e^{iy}$ para algún y . Sea $x := 1/p^s$. Aplicamos (7.2), se tiene

$$\left| \left(1 - \frac{\chi_0(p)}{p^s} \right)^3 \left(1 - \frac{\chi(p)}{p^s} \right)^4 \left(1 - \frac{\chi^2(p)}{p^s} \right) \right|^2 \leq 1.$$

Tomando la expresión sobre todos los números primos y usando la representación en producto de Euler, obtenemos la igualdad deseada. \square

Lema 7.1.10. Si $\chi \neq 1$ tenemos $|L'(s, \chi)| < \varphi(k)$ para $s \in \mathbb{R}$, $s \geq 1$.

Demostración. De la demostración del Teorema 7.1.4, tenemos

$$L'(s, \chi_0) = - \sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s} \quad \text{para } s > 1.$$

Para $t \geq 3$, $t \in \mathbb{R}$, $f(t) = \frac{\ln t}{t^s}$ es una función decreciente. Por tanto, por el Lema 7.1.8 se tiene

$$\left| \sum_{i=m}^n \frac{\chi(i) \ln i}{i^s} \right| \leq \frac{\varphi(k)}{2} \frac{\ln m}{m^s} \leq \frac{\varphi(k)}{2} \frac{\ln m}{m}.$$

En particular la serie $\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s}$ converge absolutamente para $s \geq 1$. Se sigue que para $s \geq 1$

$$\begin{aligned} |L'(s, \chi)| &= \left| \sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s} \right| \leq \frac{\chi(2) \ln 2}{2^s} + \left| \sum_{n=3}^{\infty} \frac{\chi(n) \ln n}{n^s} \right| \\ &\leq \frac{\chi(2) \ln 2}{2} + \frac{\varphi(k) \ln 3}{2} < \frac{1}{2} + \frac{\varphi(k)}{2} \leq \varphi(k). \end{aligned} \quad \square$$

Un resultado fundamental que necesitamos es:

Teorema 7.1.11. Si $\chi \neq 1$, $L(1, \chi) \neq 0$ y $\frac{L'(s, \chi)}{L'(s, \chi_0)}$ está acotada para $s > 1$ y $\chi_0 = 1$.

Demostración. Puesto que $|\sum_{i=m}^n \chi(i)| \leq \frac{\varphi(k)}{2}$, si $\chi \neq 1$ y $s \in \mathbb{R}$, $s > 1$, entonces se sigue que para toda n , $|\sum_{i=1}^n \frac{\chi(i)}{i^s}| \leq \sum_{i=1}^n \chi(i) \leq \frac{\varphi(k)}{2}$ y por tanto $|L(s, \chi)| < \varphi(k)$.

Si χ es no real, esto es, $\chi(\mathbb{Z}) \not\subseteq \mathbb{R}$, entonces $\chi^2 \neq \chi_0$ pues en caso de que $\chi^2 = \chi_0$, $\chi(\mathbb{Z}) \subseteq \{0, 1, -1\}$. En particular $|L(s, \chi^2)| < \varphi(k)$. Más aún, tomando $1 < s < 2$, se tiene

$$L(x, \chi_0) = \sum_{\substack{n=1 \\ \text{mcd}(n,k)=1}}^{\infty} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \int_1^{\infty} \frac{dx}{x^s} = \frac{s}{s-1} < \frac{2}{s-1}.$$

Por el Lema 7.1.9, se tiene

$$|L(s, \chi)| \geq \frac{1}{|L(s, \chi_0)|^{3/4}} \frac{1}{|L(x, \chi^2)|^{2/4}} > \frac{(s-1)^{3/4}}{2^{3/4}} \frac{1}{\sqrt{\varphi(k)}} > \frac{(s-1)^{3/4}}{2\sqrt{\varphi(k)}}.$$

En caso de que $L(1, \chi) = 0$, se tendría para $s > 1$

$$|L(s, \chi)| = |L(s, \chi) - L(1, \chi)| = \left| \int_1^s L'(x, \chi) dx \right| < \varphi(k)(s-1).$$

En particular para $1 < s < 2$ se seguiría que $(s-1)^{1/4} > \frac{1}{2\sqrt{\varphi(k)^{3/2}}}$ lo cual no se cumple: por ejemplo para $s = 1 + \frac{1}{16\sqrt{\varphi(k)^{3/2}}} \in (1, 2)$.

Se sigue que $L(1, \chi) \neq 0$ para χ no real.

Ahora consideremos χ real, $\chi \neq \chi_0$. Sea $f: \mathbb{N} \rightarrow \mathbb{R}$ dada por $f(n) = \sum_{d|n} \chi(d)$. Sean p_1, \dots, p_r los primos que dividen a n y que no dividen a k y sea α_i tal que $p_i^{\alpha_i} | n$ y $p_i^{\alpha_i+1} \nmid n$, $1 \leq i \leq r$. Entonces $\chi(p_i) = (-1)^{\varepsilon_i}$, $\varepsilon_i \in \{0, 1\}$, $\chi(p_i^{\alpha_i}) = (-1)^{\alpha_i \varepsilon_i}$.

Escogemos p_1, \dots, p_t con $\varepsilon_i = 1$ y p_{t+1}, \dots, p_r con $\varepsilon_i = 0$. Entonces

$$\begin{aligned} f(n) &= \sum_{i=1}^r \sum_{\beta_i=0}^{\alpha_i} \chi(p_1^{\beta_1} \cdots p_r^{\beta_r}) = \sum_{i=1}^t \sum_{\substack{\beta_i=0 \\ \text{algún } \beta_i > 0}}^{\alpha_i} \chi(p_1^{\beta_1} \cdots p_t^{\beta_t}) + \sum_{j=t+1}^r \sum_{\beta_j=0}^{\alpha_j} 1 \\ &= \sum_{i=1}^t \sum_{\beta_i=0}^{\alpha_i} (-1)^{\beta_1 + \cdots + \beta_t} + [(\alpha_{t+1} + 1) \cdots (\alpha_r + 1) - 1] \\ &\geq \sum_{i=1}^t \sum_{\beta_i=0}^{\alpha_i} (-1)^{\beta_1 + \cdots + \beta_t}. \end{aligned}$$

Podemos hacer inducción en t para ver que la suma es mayor o igual a 0. Si $t = 0$, la suma es 1 $=: h_0 > 0$. Si $t > 0$ y suponemos que $h_{t-1} := \sum_{i=1}^{t-1} \sum_{\beta_i}^{\alpha_i} (-1)^{\beta_1 + \cdots + \beta_{t-1}} \geq 0$, entonces $h_t = \sum_{\beta_t=0}^{\alpha_t} (-1)^{\beta_t} h_{t-1} = \begin{cases} h_{t-1} & \text{si } \alpha_t \text{ es par} \\ 0 & \text{si } \alpha_t \text{ es impar} \end{cases} \geq 0$.

Ahora si $n = c^2$ es un cuadrado, $h_t = h_{t-1} > 0$ y por tanto se tiene $f(n) \geq 0$ para toda $n \geq 1$ y $f(n) \geq 1$ si $n = c^2$ es un cuadrado. Sean

$$m = (4\varphi(k))^6 \quad \text{y} \quad z = \sum_{n=1}^m 2(m-n)f(n). \quad (7.3)$$

Entonces

$$z = \sum_{n=1}^m 2(m-n) \sum_{d|n} \chi(d) \underset{\substack{\uparrow \\ \frac{n}{d}=v}}{=} \sum_{n=1}^m \sum_{d|n} 2(m-vd)\chi(d) = \sum_{vd \leq m} 2(m-vd)\chi(d).$$

Se tiene que, puesto que $f(n) \geq 0$, $n \geq 1$, $f(n) \geq 1$ si $n = c^2$

$$\begin{aligned} z &\geq \sum_{v=1}^{\sqrt{m}} 2(m-v^2) \geq \sum_{v=1}^{\sqrt{m}/2} 2(m-v^2) \geq \sum_{v=1}^{\sqrt{m}/2} 2\left(m - \frac{m}{4}\right) \\ &= \frac{\sqrt{m}}{2} 2\left(\frac{3m}{4}\right) = \frac{3}{4} m^{3/2} = \frac{3}{4} (4\varphi(k))^9. \end{aligned} \quad (7.4)$$

Separamos z en dos sumandos:

$$\begin{aligned} z_1 &= \sum_{d=1}^{m^{1/3}} \sum_{m^{3/2} < v \leq m/d} 2(m-vd)\chi(d), \\ z_2 &= \sum_{v=1}^{m^{2/3}} \sum_{0 < d \leq m/v} 2(m-vd)\chi(d), \\ z &= z_1 + z_2. \end{aligned} \quad (7.5)$$

Sean $z(n)$ una función valuada en \mathbb{C} , $c \in \mathbb{N}$ y $t \geq c$. Sea $w(t) := \sum_{n=c}^t z(n)$ y definimos $w(c-1) = 0$. Para $d \geq c$ sean $\mu_d := \max_{c \leq t \leq d} |r(t)|$, y $\varepsilon_c \geq \varepsilon_{c+1} \geq \dots \geq \varepsilon_d \geq 0$. Entonces

$$\sum_{n=c}^d \varepsilon_n z_n = \sum_{n=c}^d \varepsilon_n (w(n) - w(n-1)) = \sum_{n=c}^{d-1} w(n) (\varepsilon_n - \varepsilon_{n-1}) + w(d) \varepsilon_d.$$

En particular

$$\left| \sum_{n=c}^d \varepsilon_n z(n) \right| \leq \mu_d \left(\sum_{n=c}^{d-1} (\varepsilon_n - \varepsilon_{n-1}) + \varepsilon_d \right) = v \varepsilon_c. \quad (7.6)$$

Aplicamos lo anterior a $\sum_{n=c}^d \chi(n)$. En este caso tenemos $\left| \sum_{n=c}^d \chi(n) \right| \leq \frac{\varphi(k)}{2}$ y por tanto, con $\varepsilon_n = \frac{1}{n^s}$ y $s \in \mathbb{R}$, $s > 1$, se obtiene

$$\left| \sum_{n=c}^d \frac{\chi(n)}{n^s} \right| \leq \frac{\varphi(k)}{2} \frac{1}{c^s} \leq \frac{\varphi(k)}{2c}.$$

Ahora bien, aplicando (7.6) a z_1 , obtenemos

$$z_1 \leq \left| \sum_{d=1}^{m^{1/3}} \sum_{m^{2/3} < v \leq m/d} 2(m-dv)\chi(v) \right| \leq \sum_{d=1}^{m^{1/3}} 2m \frac{\varphi(k)}{2} = m^{4/3} \varphi(k). \quad (7.7)$$

Sea ahora $\theta = \frac{m}{v} - \left[\frac{m}{v} \right]$, donde $[x]$ denota la parte entera de $x \in \mathbb{R}$. Entonces $0 \leq \theta < 1$ y se tiene

$$\begin{aligned} \sum_d (2m - 2dv) &= 2m \sum_d 1 - v \sum_d 2d = 2m \left[\frac{m}{v} \right] - v \left[\frac{m}{v} \right] \left(\left[\frac{m}{v} \right] + 1 \right) \\ &= 2m \left(\frac{m}{v} - \theta \right) - v \left(\left(\frac{m}{v} - \theta \right)^2 + \frac{m}{v} - \theta \right) \\ &= \frac{2m^2}{v} - 2m\theta - v \left(\frac{m^2}{v^2} - 2\theta \frac{m}{v} + \theta^2 + \frac{m}{v} - \theta \right) \\ &= \frac{m^2}{v} - m + v(\theta - \theta^2). \end{aligned}$$

Puesto que $0 \leq \theta < 1$, $0 \leq \theta - \theta^2 \leq \theta < 1$, y por tanto

$$\begin{aligned} z_2 &= m^2 \sum_{v=1}^{m^{2/3}} \frac{\chi(v)}{v} - m \sum_{v=1}^{m^{2/3}} \chi(v) + \sum_{v=1}^{m^{2/3}} \chi(v) v(\theta - \theta^2) \\ &\leq m^2 \left(L(1, \chi) - \sum_{v=m^{2/3}+1}^{\infty} \frac{\chi(v)}{v^s} \right) + m \frac{\varphi(k)}{2} + m^{2/3} \sum_{v=1}^{m^{2/3}} 1. \end{aligned}$$

Ahora si aplicamos la desigualdad

$$\left| \sum_{n=c}^d \frac{\chi(n)}{n^s} \right| \leq \frac{\varphi(k)}{2} \frac{1}{c^s} \leq \frac{\varphi(k)}{2c}$$

y tomando $c = m^{2/3} + 1$, $v \rightarrow \infty$ se obtiene

$$\begin{aligned} z_2 &< m^2 L(1, \chi) + m^2 \frac{\varphi(k)}{2} \frac{1}{m^{2/3}} + m^{4/3} \frac{\varphi(k)}{2} + m^{4/3} \varphi(k) \\ &= m^2 L(1, \chi) + m^{4/3} \varphi(k) \left(\frac{1}{2} + \frac{1}{2} + 1 \right) = m^2 L(1, \chi) + 2m^{4/3} \varphi(k). \quad (7.8) \end{aligned}$$

De (7.3), (7.4), (7.5), (7.7) y (7.8) obtenemos

$$\begin{aligned} \frac{3}{4} (4\varphi(k))^9 &\leq z = z_1 + z_2 \leq m^{4/3} \varphi(k) + m^2 L(1, \chi) + 2m^{4/3} \varphi(k) \\ &= m^2 L(1, \chi) + 3m^{4/3} \varphi(k) = m^2 L(1, \chi) + 3(4\varphi(k))^8 \varphi(k) \\ &= m^2 L(1, \chi) + \frac{3}{4} (4\varphi(k))^9. \end{aligned}$$

En particular $m^2 L(1, \chi) > 0$ y por tanto $L(1, \chi) > 0$. Se concluye $L(1, \chi) \neq 0$.

Esto prueba la primera parte del teorema. La segunda parte se sigue pues ya que $L(1, \chi) \neq 0$, $\frac{1}{L(s, \chi)}$ está acotada para $s \geq 1$, $s \in \mathbb{R}$. Por el Lema 7.1.10 se tiene que $L'(s, \chi)$ está acotado para $s \geq 1$, $s \in \mathbb{R}$. \square

La última parte que se necesita para el Teorema de Dirichlet es:

Teorema 7.1.12. Sean $\text{mcd}(c, k) = 1$, $n > 0$. Entonces para $s \in \mathbb{R}$, $s > 1$ tenemos:

$$-\frac{1}{\varphi(k)} \sum_{\chi \bmod k} \overline{\chi(c)} \frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n \equiv c \bmod k} \frac{\Lambda(n)}{n^s}.$$

Demostración. De la Proposición 7.1.7 se tiene que

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s}.$$

Se sigue que

$$\begin{aligned} - \sum_{\chi \bmod k} \overline{\chi(a)} \frac{L'(s, \chi)}{L(s, \chi)} &= - \sum_{\chi \bmod k} \frac{1}{\chi(c)} \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \sum_{\chi \bmod k} \frac{1}{\chi(c)} \chi(n). \end{aligned}$$

Ahora

$$\begin{aligned} \sum_{\chi \bmod k} \frac{1}{\chi(c)} \chi(n) &= \sum_{\chi \bmod k} \chi(c^{-1}n) = \sum_{\chi \in \widehat{U_k}} (\widehat{c^{-1}n})(\chi) \\ &= \begin{cases} 0 & \text{si } \widehat{c^{-1}n} \neq 1, \\ \varphi(k) & \text{si } \widehat{c^{-1}n} = 1 \end{cases} = \begin{cases} 0 & \text{si } c \not\equiv n \bmod k, \\ \varphi(k) & \text{si } c \equiv n \bmod k \end{cases}. \end{aligned}$$

Por lo tanto

$$- \sum_{\chi \bmod k} \overline{\chi(a)} \frac{L'(s, \chi)}{L(s, \chi)} = \varphi(k) \sum_{n \equiv c \bmod k} \frac{\Lambda(n)}{n^s}. \quad \square$$

Teorema 7.1.13 (Teorema de Dirichlet). Si $\text{mcd}(a, b) = 1$, $a, b \in \mathbb{N}$, entonces existen una infinidad de números primos p tales $p \equiv b \bmod a$.

Demostración. Consideremos $\widehat{U_a}$. Por el Teorema 7.1.12 con $a = k$ y $b = c$ se tiene

$$-\frac{1}{\varphi(k)} \sum_{\chi \in \widehat{U_a}} \overline{\chi(b)} \frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n \equiv b \bmod a} \frac{\Lambda(n)}{n^s}. \quad (7.9)$$

Cuando $s \rightarrow 1^+$ el lado izquierdo de (7.9) se va a ∞ pues por la Proposición 7.1.7, $-\lim_{s \rightarrow 1^+} \frac{L'(s, \chi_0)}{L(s, \chi_0)} = \infty$ y por el Teorema 7.1.11 los demás $(\varphi(a) - 1)$ términos están acotados. Por lo tanto el lado derecho de (7.9) satisface:

$$\sum_{p \equiv b \pmod{a}} \frac{\ln p}{p^s} + \sum_{\substack{p^m \equiv b \pmod{a} \\ m > 1}} \frac{\ln p}{p^{ms}} \xrightarrow{s \rightarrow 1^+} \infty.$$

Por otro lado la segunda suma permanece acotada pues

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{2 \ln n}{n^s} &> \sum_{n=2}^{\infty} \frac{\ln n}{n(n-1)} \geq \sum_p \frac{\ln p}{p(p-1)} \geq \sum_{p, m > 1} \frac{\ln p}{p^m} > \\ &> \sum_{p, m; m > 1} \frac{\ln p}{p^{ms}} \geq \sum_{\substack{p, m; m > 1 \\ p^m \equiv b \pmod{a}}} \frac{\ln p}{p^{ms}}, \quad s > 1. \end{aligned}$$

Por lo tanto $\sum_{p \equiv b \pmod{a}} \frac{\ln p}{p^s} \xrightarrow{s \rightarrow 1^+} \infty$ de donde se sigue el resultado. \square

Observación 7.1.14. Todo el desarrollo anterior lo hemos tomado de [15, 3.3].

Si suponemos conocido que la función zeta de Dedekind tiene un polo simple en $s = 1$, la demostración del Teorema 7.1.13 es casi inmediata. Primero se prueba que X es un grupo de caracteres de Dirichlet y K es el campo asociado a X , entonces

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$$

lo cual se prueba comprobando que los factores de Euler son los mismos. De ahí se sigue que $L(1, \chi) \neq 0$ para $\chi \neq 1$. A partir de aquí seguimos con los Teoremas 7.1.12 y 7.1.13.

Campos de funciones

8.1. Generalidades

En este capítulo presentamos un breve resumen, usualmente sin demostraciones, de lo que son los campos de funciones. Un desarrollo más detallado de estos campos puede consultarse en [11, 14, 68, 69, 70]. Aquí únicamente presentaremos algunos casos especiales de campos de funciones que son los que aplicaremos a lo que nos interesa que son los campos de funciones ciclotómicos (módulos de Carlitz).

Definición 8.1.1. Sea k un campo arbitrario. Un *campo de funciones* K sobre k es una extensión finitamente generada de k con grado de trascendencia 1.

Nosotros nos restringiremos al caso en que k es un campo perfecto, de hecho nuestro principal interés es cuando k es finito. En este caso, un campo de funciones K/k es un campo K de la forma $K = k(x, y)$ donde x es transcendente sobre k y y es algebraico y separable sobre $k(x)$.

Así mismo, supondremos que k es algebraicamente cerrado en K . Esto es, si $k' = \{\alpha \in K \mid \alpha \text{ es algebraico sobre } k\}$, entonces $k' = k$. En este caso k se llama *el campo de constantes* de K .

Definición 8.1.2. Sea $v: K^* \rightarrow \mathbb{Z}$ una valuación discreta de K^* que es trivial en k^* , esto es, $v(\alpha) = 0$ para $\alpha \in k^*$.

Ponemos $v(0) = \infty$ con el sobre entendido de que $x < \infty$ para toda $x \in \mathbb{Z}$. Sea $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ y $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$ el anillo de valuación de v y el ideal maximal de \mathcal{O}_v respectivamente. Entonces v también lo llamaremos “*lugar*” de K^* . Al campo $k(v) := \mathcal{O}_v/\mathfrak{p}_v$ se le llama el *campo residual* de v .

Se tiene que $[k(v) : k] < \infty$ y $[k(v) : k]$ se le llame el *grado* de v .

Recíprocamente, si $\mathcal{O} \subseteq K$ es un subanillo de K que es de valuación con $k \subseteq \mathcal{O}$ y $\text{coc } \mathcal{O} = K$, \mathcal{O} da lugar a una valuación v (que no describiremos

aquí) y si \mathfrak{p} es el ideal maximal de \mathcal{O} , se denota $k(\mathfrak{p}) = k(v)$ y $d(\mathfrak{p}) = d_K(\mathfrak{p}) = f_{\mathfrak{p}} = [k(\mathfrak{p}) : k]$ al grado de \mathfrak{p} .

Cada uno de los tres objetos: el anillo de valuación \mathcal{O} , la valuación v y el ideal máximo \mathfrak{p} de \mathcal{O} , determinan los otros dos. Todos ellos de manera indistinta los nombraremos “lugar”.

Se tiene que si v es una valuación de K , entonces $v|_{k(x)}$ es una valuación de $k(x)$ donde $x \in K \setminus k$, es decir, x es transcendente sobre k y por tanto $[K : k(x)]$ es finita.

Recíprocamente, dada una valuación v en $k(x)$, v se puede extender a una valuación en K y el número de tales extensiones es menor o igual a $[K : k(x)]$.

8.2. Valuaciones en $k(x)$

Sea $f(x) \in k[x]$ un polinomio mónico e irreducible de $k[x]$. Entonces si $\alpha(x) \in k(x)^*$, $\alpha(x)$ se puede escribir de manera única como $\alpha(x) = f(x)^s \frac{a(x)}{b(x)}$ donde $a(x), b(x) \in k[x]$ son polinomios primos relativos y $s \in \mathbb{Z}$. Entonces definimos $v_f(\alpha(x)) := s$. Se tiene que v_f es una valuación en K , asociada a, o correspondiente a, f .

Ahora sea $\beta(x) \in k(x)^*$, $\beta(x) = \frac{h(x)}{g(x)}$ con $h(x), g(x) \in k[x]$. Definimos el grado de β por: $\text{gr } \beta = \text{gr } h - \text{gr } g$. Sea $v_{\infty} : k(x)^* \rightarrow \mathbb{Z}$, $v_{\infty}(\beta(x)) = -\text{gr } \beta$. Entonces v_{∞} es otra valuación diferente a todas las valuaciones v_f , $f \in k[x]$ mónico e irreducible.

Teorema 8.2.1. *El conjunto $\{v_{\infty}, v_f \mid f(x) \in k[x] \text{ es mónico e irreducible}\}$ comprende a todas las valuaciones de K que son triviales en k .* \square

Usualmente denotaremos por $\mathfrak{p}_{\infty}, \mathfrak{p}_f$ al lugar v_{∞}, v_f respectivamente.

Notación 8.2.2. Si K es un campo de funciones, entonces $\mathbb{P}_K := \{\mathfrak{p} \mid \mathfrak{p} \text{ es lugar de } K\}$. Si $\mathfrak{p} \in \mathfrak{P}_K$ la valuación respectiva será denotada por $v_{\mathfrak{p}}$.

A continuación definimos el substituto del dominio de Dedekind \mathcal{O}_K en un campo numérico K .

Definición 8.2.3. Sea K un campo de funciones sobre k . El grupo abeliano libre generado por \mathbb{P}_K se llama *grupo de divisores* de K y denota por D_K .

Los elementos D_K se llaman *divisores*. Escribiremos D_K multiplicativamente.

Un elemento $\mathfrak{a} \in D_K$ es una expresión formal

$$\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$$

con $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathbb{P}_K$ y $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$.

Equivalentemente, $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$ donde $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ para toda $\mathfrak{p} \in \mathbb{P}_K$ y $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ para casi toda \mathfrak{p} , es decir, $v_{\mathfrak{p}}(\mathfrak{a})$ es cero para todo $\mathfrak{p} \in \mathbb{P}_K$ salvo un número finito.

El elemento identidad de D_K es el divisor $\mathfrak{N} \in D_K$ tal que $v_{\mathfrak{p}}(\mathfrak{N}) = 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$.

Los elementos de \mathbb{P}_K , es decir, los lugares, también reciben el nombre de *divisores primos*.

Se define el *grado* $\mathfrak{a} \in D_K$ por

$$d_K(\mathfrak{a}) = \sum_{\mathfrak{p} \in \mathbb{P}_K} d_K(\mathfrak{p}) v_{\mathfrak{p}}(\mathfrak{a}).$$

Dado $x \in K^*$ se tiene que existe un número finito de lugares \mathfrak{p} de K tales que $v_{\mathfrak{p}}(x) \neq 0$. Notemos que si $x \in k^*$, $v_{\mathfrak{p}}(x) = 0$ para toda $\mathfrak{p} \in \mathbb{P}_K$. Se define el *divisor principal* de $x \in K^*$ por:

$$(x)_K := \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

Se tiene que si $x \in K \setminus k$ existe al menos un lugar \mathfrak{p} de K tal que $v_{\mathfrak{p}}(x) > 0$ y otro \mathfrak{p}' tal que $v_{\mathfrak{p}'}(x) < 0$. Podemos tomar \mathfrak{p} como una extensión de \mathfrak{p}_{∞} a K .

También se tiene que si $\mathfrak{Z}_x := \prod_{v_{\mathfrak{p}}(x) > 0} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ y $\mathfrak{N}_x := \prod_{v_{\mathfrak{p}}(x) < 0} \mathfrak{p}^{-v_{\mathfrak{p}}(x)}$, entonces \mathfrak{Z}_x se llama el *divisor de ceros* de x y \mathfrak{N}_x se llama el *divisor de polos* de x .

Teorema 8.2.4. *Se tiene que si $x \in k^*$, $\mathfrak{Z}_x = \mathfrak{N}_x = \mathfrak{N}$ y si $x \in K \setminus k$, $d(\mathfrak{Z}_x) = d(\mathfrak{N}_x) = [K : k(x)]$.* \square

Corolario 8.2.5. *Para $x \in K^*$, $d_K((x)_K) = 0$.*

Demostración. Notemos que $(x)_K = \frac{\mathfrak{Z}_x}{\mathfrak{N}_x}$ y que $d_K((x)_K) = d_K(\mathfrak{Z}_x) - d_K(\mathfrak{N}_x) = 0$. \square

Sea $d_K: D_K \rightarrow \mathbb{Z}$ la función grado. Entonces d_K es un homomorfismo de grupos. Puesto que $d_K \neq 0$, $\text{im } d_K = m\mathbb{Z}$ para algún $m \in \mathbb{N}$. En particular $\text{im } d_K \cong \mathbb{Z}$. Sea $\text{nuc } d_K = D_{K,0} := \{\mathfrak{a} \in D_K \mid d_K(\mathfrak{a}) = 0\}$ el cual se llama el grupo de divisores de grado 0 de K . Además $P_K := \{(x)_K \mid x \in K^*\} \subseteq D_{K,0}$.

Se definen los siguientes grupos:

$$C_K := D_K / P_K = \text{grupo de clases de divisores de } k,$$

$$C_{K,0} := D_{K,0} / P_K = \text{grupo de clases de divisores de grado 0 de } K.$$

Notemos que si $C \in C_K$ y $\mathfrak{a}, \mathfrak{b} \in D_K$ son tales que $\mathfrak{a}, \mathfrak{b} \in C$, entonces $\mathfrak{a} = \mathfrak{b}(x)_K$ para algún $x \in K$. En particular $d_K(\mathfrak{a}) = d_K(\mathfrak{b})$. Por tanto podemos definir el *grado* de C por: $\tilde{d}_K(C) := d_K(\mathfrak{a})$ para $\mathfrak{a} \in C$. Se tiene que

$\tilde{d}_K: C_K \rightarrow \mathbb{Z}$ también es un homomorfismo de grupos con $\text{im } \tilde{d}_K = \text{im } d_K = m\mathbb{Z}$ y núc $\tilde{d}_K = C_{K,0}$. En adelante pondremos $\tilde{d}_K = d_K$.

Se tienen las siguientes sucesiones exactas de grupos abelianos:

$$\begin{aligned} 1 \longrightarrow D_{K,0} \longrightarrow D_K \xrightarrow{d_K} \text{im } d_K \cong \mathbb{Z} \longrightarrow 0, \\ 1 \longrightarrow C_{K,0} \longrightarrow C_K \xrightarrow{d_K} \text{im } d_K \cong \mathbb{Z} \longrightarrow 0, \\ 1 \longrightarrow P_K \longrightarrow D_{K,0} \longrightarrow C_{K,0} \longrightarrow 0, \\ 1 \longrightarrow P_K \longrightarrow D_K \longrightarrow C_K \longrightarrow 0, \\ 1 \longrightarrow k^* \longrightarrow K^* \longrightarrow P_K \longrightarrow 1. \\ \quad \quad \quad x \longrightarrow (x)_K \end{aligned}$$

Puesto que \mathbb{Z} es un grupo abeliano libre, en particular proyectivo, se tiene

$$\begin{aligned} C_K &\cong C_{K,0} \oplus \text{im } d_K \cong C_{K,0} \oplus \mathbb{Z}, \\ D_K &\cong D_{K,0} \oplus \text{im } d_K \cong D_{K,0} \oplus \mathbb{Z}. \end{aligned}$$

Los isomorfismos anteriores los podemos explicitar de la siguiente forma. Sea $\mathfrak{a}_1 \in D_K$ tal que $d_K(\mathfrak{a}_1) = m$ donde $\text{im } d_K = m\mathbb{Z}$ y $m > 0$. Sea $\mathfrak{a} \in D_K$ arbitrario. Entonces $d_K(\mathfrak{a}) = tm$. Sea $\mathfrak{a}_0 := \mathfrak{a}\mathfrak{a}_1^{-t}$. Entonces $d(\mathfrak{a}_0) = 0$ y $\varphi: D_K \rightarrow D_{K,0} \oplus \mathbb{Z}$ es el isomorfismo buscado. Similarmente para C_K .

$$\mathfrak{a} \mapsto (\mathfrak{a}_0, t)$$

En general $m > 1$. Sin embargo cuando k es finito se tiene que $m = 1$.

8.3. Reparticiones y diferenciales

Sea $\mathfrak{p} \in \mathbb{P}_K$ y sea $K_{\mathfrak{p}}$ la completación de K con respecto a la topología dada por la métrica: $\|x\|_{\mathfrak{p}} := e^{-v_{\mathfrak{p}}(x)}$ donde entendemos $e^{-\infty} = 0$, es decir, $\|0\|_{\mathfrak{p}} = 0$.

Definición 8.3.1. Una *repartición* o *adèle* de K es una función

$$\varphi: \mathbb{P}_K \longrightarrow \bigcup_{\mathfrak{p} \in \mathbb{P}_K} K_{\mathfrak{p}}$$

tal que

- (1) $\varphi(\mathfrak{p}) \in K_{\mathfrak{p}} \ \forall \ \mathfrak{p} \in \mathbb{P}_K$,
- (2) $v_{\mathfrak{p}}(\varphi(\mathfrak{p})) \geq 0$ para casi toda $\mathfrak{p} \in \mathbb{P}_K$.

Equivalentemente una repartición es una sucesión $\xi = \{\xi_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathbb{P}_K}$ tal que $\xi_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}$ para casi toda $\mathfrak{p} \in \mathbb{P}_K$. Se define

$$v_{\mathfrak{p}}(\xi) := v_{\mathfrak{p}}(\xi_{\mathfrak{p}}).$$

Notación 8.3.2. \mathfrak{X}_K o Λ_K denota el espacio de todas las reparticiones de K .

\mathfrak{X}_K tiene una estructura de K -álgebra con las operaciones

$$\begin{aligned}(\theta\xi)_{\mathfrak{p}} &:= \theta_{\mathfrak{p}}\xi_{\mathfrak{p}}, \\(\theta + \xi)_{\mathfrak{p}} &:= \theta_{\mathfrak{p}} + \xi_{\mathfrak{p}}, \\(x\xi)_{\mathfrak{p}} &:= x\xi_{\mathfrak{p}},\end{aligned}$$

para cualesquiera $\theta, \xi \in \mathfrak{X}_K$, $x \in K$ y $\mathfrak{p} \in \mathbb{P}_K$ y se tiene que $\varphi: K \rightarrow \mathfrak{X}_K$ dada por $\varphi(x) := \xi_x$ donde $(\xi_x)_{\mathfrak{p}} = x$ para toda $\mathfrak{p} \in \mathbb{P}_K$ es un monomorfismo de anillos. De esta forma podemos considerar $K \subseteq \mathfrak{X}_K$.

Sea \mathfrak{a} un divisor $\mathfrak{a} \in D_K$ y ξ una repartición de K . Entonces decimos que \mathfrak{a} divide a ξ y ponemos $\mathfrak{a}|\xi$ si $v_{\mathfrak{p}}(\xi) = v_{\mathfrak{p}}(\xi_{\mathfrak{p}}) \geq v_{\mathfrak{p}}(\mathfrak{a})$ para toda $\mathfrak{p} \in \mathbb{P}_K$.

Definimos $\mathfrak{X}_K(\mathfrak{a}) = \Lambda_K(\mathfrak{a}) = \{\xi \in \mathfrak{X}_K \mid \mathfrak{a}|\xi\}$. Entonces $\mathfrak{X}_K(\mathfrak{a})$ es un k -subespacio vectorial de \mathfrak{X}_K .

Definición 8.3.3. Una *diferencial* (de Weil) de K es una función k -lineal (k -funcional) $\omega: \mathfrak{X}_K \rightarrow k$ tal que existe un divisor tal que $\mathfrak{X}_K(\mathfrak{a}) + K \subseteq \text{núc } \omega$.

En este caso decimos que \mathfrak{a}^{-1} divide a ω y ponemos $\mathfrak{a}^{-1}|\omega$.

Por otro lado el espacio de diferenciales \mathfrak{D}_K forma un K -espacio vectorial con las operaciones de suma de funciones y donde para $x \in K$, $\omega \in \mathfrak{D}$, $(x\omega)(\xi) := \omega(x\xi)$, $\xi \in \mathfrak{X}_K$.

De hecho $\dim_K \mathfrak{D} = 1$, es decir, si ω_0 es cualquier diferencial no cero, entonces toda diferencial $\omega \in \mathfrak{D}$ puede escribirse de manera única como $\omega = x\omega_0$, para algún $x \in K$.

Ahora bien, si ω es una diferencial no cero existe un único divisor $(\omega)_K \in \mathfrak{D}_K$ tal que para un divisor arbitrario $\mathfrak{a} \in D_K$ se tiene

$$\mathfrak{a}|\omega \iff \mathfrak{a} | (\omega)_K,$$

esto es,

$$\mathfrak{X}_K(\mathfrak{a}^{-1}) + K \subseteq \text{núc } \omega \iff v_{\mathfrak{p}}((\omega)_K) \geq v_{\mathfrak{p}}(\mathfrak{a}) \quad \forall \mathfrak{p} \in \mathbb{P}_K.$$

El divisor $(\omega)_K$ se construye de la siguiente forma. Dado $\omega \neq 0$, si $\mathfrak{a}|\omega$ entonces se tiene que $d_K(\mathfrak{a})$ está acotado superiormente. Entonces $(\omega)_K$ es el divisor de máximo grado que divide a ω .

Ahora bien, si $\mathfrak{D}_K(\mathfrak{a}) := \{\omega \mid \omega = 0 \text{ o } \omega \neq 0 \text{ y } \mathfrak{a}|\omega\}$, entonces $\mathfrak{D}_K(\mathfrak{a})$ es un k -espacio vectorial y se tiene que $\mathfrak{D}_K(\mathfrak{a})$ y $\frac{\mathfrak{X}_K}{\mathfrak{X}_K(\mathfrak{a}^{-1}) + K}$ son isomorfos. De hecho el mapeo k -bilineal

$$\begin{aligned}\varphi: \mathfrak{D}_K(\mathfrak{a}) \times \frac{\mathfrak{X}_K}{\mathfrak{X}_K(\mathfrak{a}^{-1}) + K} &\longrightarrow k \\(\omega, \bar{\xi}) &\longmapsto \omega(\xi)\end{aligned}$$

es no degenerado y se tiene que $\mathfrak{D}_K(\mathfrak{a})$ es de dimensión finita.

Para ver la dimensión de estos espacios, consideremos:

Definición 8.3.4. Sea $\mathfrak{a} \in D_K$. Se define $L_K(\mathfrak{a}) = \{x \in K \mid x = 0 \text{ o } x \neq 0 \text{ y } \mathfrak{a} \mid (x)_K\} = \{x \in K \mid v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{a}) \ \forall \ \mathfrak{p} \in \mathbb{P}_K\}$.

Se tiene que $L_K(\mathfrak{a})$ es k -espacio vectorial.

Teorema 8.3.5. Para todo $\mathfrak{a} \in D_K$, $L_K(\mathfrak{a})$ es un k -espacio vectorial de dimensión finita y denotamos por $\ell_K(\mathfrak{a})$ la dimensión de $L_K(\mathfrak{a})$: $\ell_K(\mathfrak{a}) = \dim_k L_K(\mathfrak{a})$. \square

Notemos que si $d_K(\mathfrak{a}) > 0$, entonces $L_K(\mathfrak{a}) = \{0\}$ y $\ell_K(\mathfrak{a}) = 0$.

Se tiene la sucesión exacta de k -espacios vectoriales donde $\mathfrak{a} \mid \mathfrak{b}$

$$0 \longrightarrow \frac{L_K(\mathfrak{a})}{L_K(\mathfrak{b})} \longrightarrow \frac{\mathfrak{X}_K(\mathfrak{a})}{\mathfrak{X}_K(\mathfrak{b})} \longrightarrow \frac{\mathfrak{X}_K(\mathfrak{a}) + K}{\mathfrak{X}_K(\mathfrak{b}) + K} \longrightarrow 0.$$

Un resultado central en la teoría de las funciones algebraicas es el Teorema de Riemann–Roch, el cual enunciamos a continuación.

Teorema 8.3.6 (Riemann–Roch). Sea K/k cualquier campo de funciones. Existe un entero no negativo $g_K \geq 0$ que depende únicamente de K , llamado el género de K tal que

(I) (Riemann) Para cualquier divisor $\mathfrak{a} \in D_K$ se tiene

$$\ell_K(\mathfrak{a}) + d_K(\mathfrak{a}) \geq 1 - g_K.$$

Es decir $\delta_K(\mathfrak{a}^{-1}) := \ell_K(\mathfrak{a}) + d_K(\mathfrak{a}) + g_K - 1 \geq 0$.

(II) Se tiene

$$\begin{aligned} \delta_K(\mathfrak{a}) &= \dim_k \mathfrak{D}_K(\mathfrak{a}) = \dim_k \frac{\mathfrak{X}_K}{\mathfrak{X}(\mathfrak{a}^{-1}) + K} \\ &= \ell_K(\mathfrak{a}^{-1}) + d_K(\mathfrak{a}^{-1}) + g_K - 1. \end{aligned}$$

(III) Se tiene $\delta_K(\mathfrak{a}) = \ell_K(\mathfrak{a}(\omega)_K^{-1})$ donde ω es cualquier diferencial no cero.

(IV) (Riemann–Roch) Se tiene que para cualquier divisor \mathfrak{a} y cualquier diferencial no cero ω ,

$$\ell_K(\mathfrak{a}^{-1}) = d_K(\mathfrak{a}) - g_K + 1 + \ell_K(\mathfrak{a}(\omega)_K^{-1}). \quad \square$$

Como consecuencia del Teorema de Riemann–Roch tenemos

Corolario 8.3.7.

(I) $\delta_K(\mathfrak{N}) = g_K$.

(II) Si $\omega \in \mathfrak{D}_K$, $\omega \neq 0$, $d_K((\omega)_K) = 2g_K - 2$.

(III) Si $d_K(\mathfrak{a}) > 2g_K - 2$, $\ell_K(\mathfrak{a}^{-1}) = d_K(\mathfrak{a}) - g_K + 1$.

(IV) Si $\mathfrak{p} \in \mathbb{P}_K$ y $n \in \mathbb{N}$, $n > 2g_K - 1$, existe $x \in K$ tal que $\mathfrak{N}_x = \mathfrak{p}^n$, esto es, $(x)_K = \frac{\mathfrak{a}}{\mathfrak{p}^n}$ con \mathfrak{a} un divisor entero y primo relativo a \mathfrak{p} , esto es, $v_{\mathfrak{p}}(\mathfrak{a}) = 0$. \square

8.4. Extensiones de Galois

Definición 8.4.1. Sean K/k y L/ℓ dos campos de funciones. Decimos que L es una *extensión* de K si $K \subseteq L$ y $\ell \cap K = k$.

Si $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ tal que \mathfrak{P} es una extensión de \mathfrak{p} . Se define el *grado relativo* por

$$d_{L/K}(\mathfrak{P}|\mathfrak{p}) = [\ell(\mathfrak{P}) : k(\mathfrak{p})].$$

Notemos que puesto que se tiene el diagrama

$$\begin{array}{ccc} k(\mathfrak{p}) & \text{---} & \ell(\mathfrak{P}) \\ | & & | \\ k & \text{---} & \ell \end{array}$$

y $d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$, $d_L(\mathfrak{P}) = [\ell(\mathfrak{P}) : \ell]$, se sigue $d_{L/K}(\mathfrak{P}|\mathfrak{p})d_K(\mathfrak{p}) = d_L(\mathfrak{P})[\ell : k]$ (finito o infinito).

Puesto que $d_K(\mathfrak{p})$ y $d_L(\mathfrak{P})$ son finitos, se tiene que $d_{L/K}(\mathfrak{P}|\mathfrak{p}) < \infty \iff [\ell : k] < \infty$.

Proposición 8.4.2. Sea L/ℓ una extensión de K/k . Sea $\mathfrak{p} \in \mathbb{P}_K$. Entonces el número de extensiones de la valuación $v_{\mathfrak{p}}$ a L es finito.

Demostración. Por el Teorema de Riemann–Roch, existe $x \in K$ tal que $\mathfrak{N}_{x,K} = \mathfrak{p}^n$ para algún $n \in \mathbb{N}$. Ahora $\mathfrak{P} \in \mathbb{P}_L$ extiende a \mathfrak{p} si y sólo si $v_{\mathfrak{P}}(x) < 0$ lo cual es equivalente a que $\mathfrak{P}|\mathfrak{N}_{x,L}$. Este último número es finito. \square

Definición 8.4.3. Sea $\mathfrak{P} \in \mathbb{P}_L$ y sea \mathfrak{p} la restricción \mathfrak{P} a K . Esto es, $v_{\mathfrak{P}}|_K$ es equivalente a $v_{\mathfrak{p}}$. Ahora bien $v_{\mathfrak{P}} : L^* \rightarrow \mathbb{Z}$ es suprayectiva pero $v_{\mathfrak{P}}|_{K^*} : K^* \rightarrow \mathbb{Z}$ no necesariamente lo es. Se define *índice de ramificación* de \mathfrak{P} sobre \mathfrak{p} como el número natural $e = e_{L/K}(\mathfrak{P}|\mathfrak{p})$ tal que $v_{\mathfrak{P}}(\alpha) = ev_{\mathfrak{p}}(\alpha)$ para $\alpha \in K$.

Definición 8.4.4. Si L/ℓ es una extensión de K/k y si $\mathfrak{p} \in \mathbb{P}_K$, entonces si $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ son todas las extensiones de K a L se define la *conorma* de \mathfrak{p} a L por

$$\text{con}_{K/L} \mathfrak{p} = \mathfrak{P}_1^{e_{L/K}(\mathfrak{P}_1|\mathfrak{p})} \dots \mathfrak{P}_h^{e_{L/K}(\mathfrak{P}_h|\mathfrak{p})}.$$

Si $\mathfrak{a} \in D_K$ es un divisor, $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$ se define la conorma de \mathfrak{a} por

$$\text{con}_{K/L}(\mathfrak{a}) = \prod_{i=1}^r \text{con}_{K/L}(\mathfrak{p}_i)^{\alpha_i}.$$

Teorema 8.4.5. Para cualquier extensión L/ℓ de K/k , finita o infinita, se tiene

$$[L : K] = \sum_{i=1}^h e_{L/K}(\mathfrak{P}_i|\mathfrak{p}) d_{L/K}(\mathfrak{P}_i|\mathfrak{p}). \quad \square$$

Cuando L/K es una extensión de Galois se tiene que $d_{L/K}(\mathfrak{P}_i|\mathfrak{p}) = d_{L/K}(\mathfrak{P}_j|\mathfrak{p})$ y $e_{L/K}(\mathfrak{P}_i|\mathfrak{p}) = e_{L/K}(\mathfrak{P}_j|\mathfrak{p})$ para todo $1 \leq i, j \leq h$. Sean

$$f := d_{L/K}(\mathfrak{P}_i|\mathfrak{p}), \quad e = e_{L/K}(\mathfrak{P}_i|\mathfrak{p}), \quad 1 \leq i \leq h.$$

Entonces el Teorema 8.4.5 toma la forma

$$[L : K] = efh.$$

Definición 8.4.6. Sea L/K una extensión de Galois con grupo de Galois $G = \text{Gal}(L/K)$. Sea $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ una extensión de \mathfrak{p} . Se define

- (i) $D = D_{L/K}(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\} =$ grupo de descomposición de L/K .
- (ii) $I = I_{L/K}(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G \mid \sigma x \equiv x \pmod{\mathfrak{P}} \forall x \in \mathcal{O}_{\mathfrak{P}}\} =$ grupo de inercia de L/K .

Como en el caso de campos numéricos, se tiene que

$$\begin{aligned} I \subseteq D, \quad |I| = e = e_{L/K}(\mathfrak{P}|\mathfrak{p}), \quad |D| = ef \quad \text{donde} \quad f = d_{L/K}(\mathfrak{P}|\mathfrak{p}), \\ D/I \cong \text{Gal}(\ell(\mathfrak{P}/k(\mathfrak{p})), \\ D \cong \text{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}), \end{aligned}$$

donde $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ son las completaciones de L y K en \mathfrak{P} y \mathfrak{p} respectivamente.

8.5. Diferente, discriminante y ramificación

Sea L/K una extensión separable de campos de funciones, \mathfrak{P} un lugar de L y $\mathfrak{p} := \mathfrak{P}|_K$. Sean $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ las respectivas completaciones. Se tiene que $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = e_{L/K}(\mathfrak{P}|\mathfrak{p})d_{L/K}(\mathfrak{P}|\mathfrak{p})$. Sea \tilde{L} la cerradura de Galois de L/K y sea \mathfrak{P} un lugar en \tilde{L} sobre \mathfrak{P} .

Sea $\mathcal{O}_{\mathfrak{P}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) \geq 0\}$ la completación de $\mathcal{O}_{\mathfrak{P}}$ y $\hat{\mathfrak{P}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) > 0\}$ la completación de \mathfrak{p} . Si $\text{Tr} = \text{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ denota la traza de $L_{\mathfrak{P}}$ a $K_{\mathfrak{p}}$ se tiene:

Teorema 8.5.1. *Existe $m \in \mathbb{Z}$, $m \geq 0$ tal que si $x \in L_{\mathfrak{P}}$ satisface $v_{\mathfrak{P}}(x) \geq -m$, entonces $v_{\mathfrak{p}}(\text{Tr } x) \geq 0$ y existe $x_0 \in L_{\mathfrak{P}}$ tal que $v_{\mathfrak{P}}(x_0) < -m$ y $v_{\mathfrak{p}}(\text{Tr } x_0) < 0$.* \square

Definición 8.5.2. El máximo entero no negativo que satisface las condiciones del Teorema 8.5.1 se denota por $m(\mathfrak{P})$ y es llamado el *exponente diferencial* de \mathfrak{P} con respecto a K .

Teorema 8.5.3. *Se tiene que $m(\mathfrak{P}) \geq e - 1 = e_{L/K}(\mathfrak{P}|\mathfrak{p}) - 1$. Además, puesto que k es perfecto, $m(\mathfrak{P}) > e - 1$ si y sólo si la característica de k divide a e . En particular $m(\mathfrak{P}) = 0$ si \mathfrak{P} no es ramificado.* \square

Como en el caso numérico, se define que \mathfrak{P} es *moderadamente ramificado* si $p \nmid e$ y *salvajemente ramificado* si $p|e$, donde p es la característica de k .

Teorema 8.5.4. *Se tiene que $m(\mathfrak{P}) = 0$ salvo un número finito de lugares \mathfrak{P} .*
□

Definición 8.5.5. El divisor $\mathfrak{D}_{L/K} := \prod_{\mathfrak{P} \in \mathbb{P}_L} \mathfrak{P}^{m(\mathfrak{P})}$ se llama el *diferente de la extensión L/K* y se tiene que $\mathfrak{P} | \mathfrak{D}_{L/K} \iff \mathfrak{P}$ es ramificado.

El *discriminante* $\mathfrak{d}_{L/K}$ de la extensión L/K se define como la norma del diferente: $\mathfrak{d}_{L/K} := N_{L/K}(\mathfrak{D}_{L/K})$.

Sea L/K una extensión separable de campos de funciones. Sea $\mathfrak{p} \in \mathbb{P}_K$ dado. Por el Teorema de Riemann–Roch existe $x \in K$ tal que $\mathfrak{N}_x = \mathfrak{p}^n$ para algún $n \geq 1$. Entonces $k[x]$ es un dominio Dedekind y sean \mathcal{O}_K y \mathcal{O}_L las cerraduras enteras de $k[x]$ en K y L respectivamente. Entonces \mathcal{O}_K y \mathcal{O}_L son dominios Dedekind. Se puede definir el diferente de los dominios \mathcal{O}_L y \mathcal{O}_K de la manera usual; esto es,

$$\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}^{-1} := \{x \in L \mid \text{Tr}_{L/K}(xy) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_L\}.$$

Entonces se tiene que si identificamos los ideales primos de \mathcal{O}_L con los lugares de L que no están sobre \mathfrak{p} , se tiene

$$\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} = \prod_{\substack{\mathfrak{P} \in \mathbb{P}_L \\ \mathfrak{P} \nmid \mathfrak{p}}} \mathfrak{P}^{m(\mathfrak{P})},$$

es decir, los exponentes $m(\mathfrak{P})$ son los mismos que los de la Definición 8.5.2 y en $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ solo faltan los primos que dividen a \mathfrak{p} .

Es más fácil estudiar $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ que $\mathfrak{D}_{L/K}$ y para completar la información sobre $\mathfrak{D}_{L/K}$ podemos tomar otro lugar $\mathfrak{p}' \neq \mathfrak{p}$ y repetir el proceso para obtener los exponentes $m(\mathfrak{P})$ de los lugares \mathfrak{P} de L sobre \mathfrak{p} .

Para dominios Dedekind, tenemos la siguiente forma para calcular diferentes.

Teorema 8.5.6. *Sea A un dominio Dedekind, $K := \text{coc } A$ el campo de cocientes y L/K una extensión finita y separable de K . Sea B la cerradura entera de A en L . Entonces B es un dominio Dedekind y*

- (I) *Si existe $\alpha \in B$ tal que $B = A[\alpha]$ entonces $\mathfrak{D}_{B/A} = \langle f'(\alpha) \rangle$ donde $f(x) = \text{Irr}(\alpha, x, K)$.*
- (II) *En general se tiene*

$$\mathfrak{D}_{B/A} = \langle f'(\alpha) \mid \alpha \in B, L = K(\alpha) \text{ y } f(x) = \text{Irr}(\alpha, x, K) \rangle. \quad \square$$

8.6. Formula de Riemann–Hurwitz

Sea L/ℓ una extensión finita de K/k .

Definición 8.6.1. Sea $\xi \in \mathfrak{X}_K$. Se define la *cotaza* de ξ , denotada por $\text{cotr}_{K/L} \xi$, como la repartición $\theta \in \mathfrak{X}_L$ dada como: si $\mathfrak{P} \in \mathbb{P}_L$, $\mathfrak{P}|_K = \mathfrak{p}$ y puesto que $K_{\mathfrak{p}} \subseteq L_{\mathfrak{P}}$ se define $\theta_{\mathfrak{P}} := \xi_{\mathfrak{p}}$.

Si $\Omega \in \mathfrak{D}_L$ es una diferencial de L , se define la *traza* de Ω , y se denota por $\text{tr}_{L/K} \Omega$ como la diferencial ω definida por:

$$\omega: \mathfrak{X}_K \rightarrow k, \quad \omega(\xi) := \Omega(\text{cotr}_{K/L} \xi).$$

Se tiene que si $\xi \in \mathfrak{X}_K$, $\Omega \in \mathfrak{D}_L$, entonces $\text{cotr}_{K/L} \xi \in \mathfrak{X}_L$ y que $\text{tr}_{L/K} \Omega \in \mathfrak{D}_K$.

Definición 8.6.2. Si $\theta \in \mathfrak{X}_L$ definimos la *traza* de θ , denotada por $\text{tr}_{L/K} \theta$ como ξ donde para $\mathfrak{p} \in \mathbb{P}_K$:

$$\xi_{\mathfrak{p}} = \sum_{i=1}^h \text{tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}} \theta_{\mathfrak{P}_i}$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ son los lugares sobre \mathfrak{p} . Se tiene que $\xi = \text{tr}_{L/K} \theta \in \mathfrak{X}_K$.

En el caso anterior, a la operación cotaza de reparticiones le asociamos la operación traza de diferenciales. Recíprocamente a la operación traza de reparticiones queremos asociarle una operación cotaza de diferenciales. En este punto tenemos el problema que únicamente obtenemos k -linealidad y no ℓ -linealidad. Por lo pronto nos restringimos al caso “geométrico”, esto es, cuando $\ell = k$.

Definición 8.6.3. Sea L/K una extensión finita y geométrica de campos de funciones, es decir, $k = \ell$. Sea $\omega \in \mathfrak{D}_K$. Definimos la *cotaza* de ω , denotada por $\text{cotr}_{K/L} \omega$, por Ω donde para $\xi \in \mathfrak{X}_L$, $\Omega(\xi) = \omega(\text{tr}_{L/K} \xi)$.

Se tiene:

Teorema 8.6.4. Si L/K es geométrica y finita, entonces para $\omega \in \mathfrak{D}_K$, $\text{cotr}_{K/L} \omega \in \mathfrak{D}_L$. Más aún si L/K es separable entonces $\text{cotr}_{K/L} \omega \neq 0$ para $\omega \neq 0$ y se tiene que

$$(\text{cotr}_{K/L} \omega)_L = \mathfrak{D}_{L/K} \text{con}_{K/L}(\omega)_K. \quad \square$$

El Teorema 8.6.4 junto con el Corolario 8.3.7 (II) obtenemos la fórmula de Riemann–Hurwitz:

Teorema 8.6.5 (Riemann–Hurwitz). Sea L/K una extensión finita, separable y geométrica. Entonces

$$2g_L - 2 = [L : K](2g_K - 2) + d_L(\mathfrak{D}_{L/K}). \quad (8.1)$$

Demostración. Se tiene que \mathfrak{a} es un divisor de K entonces $d_L(\text{con}_{K/L}(\mathfrak{a})) = [L : K]d_K(\mathfrak{a})$. Por tanto de $(\Omega)_L = \text{con}_{K/L}(\omega)_K \mathfrak{D}_{L/K}$ obtenemos que

$$d_L((\Omega)_L) = d_L(\text{con}_{K/L}(\omega)_K) + d_L(\mathfrak{D}_{L/K})$$

la cual es precisamente (8.1). \square

Como en el caso numérico, tenemos los grupos de ramificación y su relación con el diferente.

Definición 8.6.6. Sea $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ sobre \mathfrak{p} . Sean $G_{-2} := G$, $G_{-1} := D_{L/K}(\mathfrak{P}|\mathfrak{p})$, $G_0 := I_{L/K}(\mathfrak{P}|\mathfrak{p})$ y para $i \geq -1$, $i \in \mathbb{Z}$ se define el i -ésimo grupo de ramificación G_i por:

$$G_i := \{\sigma \in G_{-1} \mid v_{\mathfrak{P}}(\sigma a - a) \geq i + 1 \text{ para toda } a \in \mathcal{O}_L\}.$$

Se tiene que G_i es un subgrupo normal de $G_{-1} = D(\mathfrak{P}|\mathfrak{p})$, que $G_{i+1} \subseteq G_i$ para toda $i \in \mathbb{Z}$, $i \geq -1$ y que existe i_0 tal que $G_{i_0} = \{\text{Id}\}$.

Si $\sigma \in G_{-1}$, $\sigma \neq \text{Id}$, existe i tal que $\sigma \in G_i \setminus G_{i+1}$. Se pone $i_{G_{-1}} = i$. Si $\sigma = \text{Id}$, definimos $i_{G_{-1}}(\sigma) = i_{G_{-1}}(\text{Id}) = \infty$. Notemos que

$$i_{G_{-1}}(\sigma) \geq j + 1 \iff \sigma \in G_j \quad \text{y que} \quad \sum_{\substack{\sigma \neq \text{Id} \\ \sigma \in G_{-1}}} i_{G_{-1}}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1).$$

Se tiene:

Teorema 8.6.7. Si $m(\mathfrak{P})$ es el exponente diferencial de \mathfrak{P} , entonces

$$m(\mathfrak{P}) = \sum_{\substack{\sigma \in G_{-1} \\ \sigma \neq \text{Id}}} i_{G_{-1}}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1). \quad \square$$

Campos de funciones ciclotómicos

9.1. Campos de funciones congruentes

Se tiene que hay muchas similitudes entre los campos numéricos y los campos de funciones. Cuando en estos últimos el campo de constantes es finito, los campos residuales también son finitos y nos permiten avanzar en esta analogía. Sin embargo, de entrada, hay diferencias fundamentales. Si K es un campo numérico y \mathfrak{p} es un ideal primo en \mathcal{O}_K , se tiene que $\mathcal{O}_K/\mathfrak{p}$ es finito y en particular de característica finita siendo que el campo K es de característica 0, esto es K y $\mathcal{O}_K/\mathfrak{p}$ tienen características diferentes.

Por otro lado, si K/k es un campo de funciones y $\mathfrak{p} \in \mathbb{P}_K$, entonces $k(\mathfrak{p})$ es una extensión finita de k y por tanto k , $k(\mathfrak{p})$ y K tienen la misma característica.

Cuando estudiamos \mathbb{Q} , tenemos que \mathbb{Q} es el campo de cocientes de \mathbb{Z} . El análogo a \mathbb{Q} sería un campo de funciones racionales $k(x)$ y el análogo a \mathbb{Z} sería $k[x]$ pues $k(x)$ es el campo de cocientes de $k[x]$ siendo además que tanto \mathbb{Z} como $k[x]$ son anillos euclidianos. Sin embargo, a pesar de ser, en cierto sentido, bastante parecidos, hay diferencias esenciales.

Por ejemplo, para $a, b, c, d \in k$ con $ad - bc \neq 0$, se tiene que $k(\frac{ax+b}{cx+d}) = k(x)$, y por tanto el anillo de polinomios de $k(y) = k(\frac{ax+b}{cx+d})$ donde $y = \frac{ax+b}{cx+d}$, es $k[y]$ el cual, a pesar de ser isomorfo a $k[x]$, no es igual siendo que los campos de cocientes si son iguales. Esto no sucede en \mathbb{Z} , es decir, si R es un subanillo de \mathbb{Q} isomorfo a \mathbb{Z} como anillo, entonces $R = \mathbb{Z}$. Otra diferencia es de que si F es un campo que contiene a \mathbb{Q} y es isomorfo a \mathbb{Q} , entonces $F = \mathbb{Q}$. Esto tampoco sucede con los campos de funciones racionales. De hecho si $n \in \mathbb{N}$, entonces $k(x^n) \cong k(x) \cong k(x^{1/n})$ como campos pero $k(x^n) \subseteq k(x) \subseteq k(x^{1/n})$ y $[k(x^{1/n}) : k(x)] = n$ y $[k(x) : k(x^n)] = n$.

Definición 9.1.1. Un campo de funciones K/k se llama *congruente* si k es finito, $|k| = q$, $k \cong \mathbb{F}_q$.

Teorema 9.1.2. Si K/k es un campo de funciones congruente, ℓ es una extensión finita de k y $L := K\ell$, entonces el campo de constantes de L es ℓ .

Demostración. Escribamos $\ell = k(\xi)$ con $[\ell : k] = f$. Entonces $\ell \cong \mathbb{F}_{q^f}$ e $\text{Irr}(\xi, x, k) | x^{q^f} - x = \prod_{\alpha \in \ell} (x - \alpha)$. Ahora bien, $L = K\ell = Kk(\xi) = K(\xi)$ con $\text{Irr}(\xi, x, K) | \text{Irr}(\xi, x, k)$. En particular $\text{Irr}(\xi, x, K) \in K[x] \cap \ell[x] = k[x]$. Por lo tanto

$$\begin{aligned} \text{Irr}(\xi, x, K) &= \text{Irr}(\xi, x, k) \quad \text{y} \\ [L : K] &= \text{gr Irr}(\xi, x, K) = \text{gr Irr}(\xi, x, k) = [\ell : k]. \end{aligned}$$

Sea ℓ' el campo de constantes de L , $\ell \subseteq \ell'$. Por tanto $L = K\ell'$. Imitando el paso que acabamos de realizar, tendríamos que $[\ell' : k] = [L : K] = [\ell : k] = f$ lo cual implica que $\ell' = \ell$. \square

Teorema 9.1.3. *Si $L = K\ell$ como antes, $g_K = g_L$, no hay primos ramificados y $\ell(\mathfrak{P}) = \ell k(\mathfrak{p})$ donde $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ está sobre \mathfrak{p} .* \square

Sean K , L , k y ℓ como antes. Sea $\mathfrak{p} \in \mathbb{P}_K$ y sean $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ los lugares de L sobre \mathfrak{p} . Ahora bien, ℓ/k siempre es una extensión de Galois, de hecho cíclica: $\text{Gal}(\ell/k) \cong \mathbb{Z}/f\mathbb{Z} \cong C_f$. Por tanto L/K es una extensión de Galois y $d_{L/K}(\mathfrak{P}_i | \mathfrak{p}) = d$, $1 \leq i \leq h$.

Por los Teoremas 8.4.5 y 9.1.3 se sigue que

$$[L : K] = [\ell : k] = f = dh.$$

Ahora bien, si $r = d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$, entonces $k(\mathfrak{p}) \cong \mathbb{F}_{q^r}$ y si $s = d_L(\mathfrak{P}_i) = [\ell(\mathfrak{P}_i) : \ell]$, entonces $\ell(\mathfrak{P}_i) \cong \mathbb{F}_{q^{fs}}$.

Se tiene que $k(\mathfrak{p})\ell \cong \mathbb{F}_{q^r}\mathbb{F}_{q^f} = \mathbb{F}_{q^{[r,f]}} = \mathbb{F}_{q^{fs}} \cong \ell(\mathfrak{P}_i)$. Por tanto $fs = [r, f] = \frac{rf}{(r,f)}$ y $s = \frac{f}{(r,f)}$. Esto es,

$$d_L(\mathfrak{P}_i) = s = \frac{d_K(\mathfrak{p})}{(d_K(\mathfrak{p}), f)}.$$

Por otro lado tenemos $d_{L/K}(\mathfrak{P}_i | \mathfrak{p})d_K(\mathfrak{p}) = d_L(\mathfrak{P}_i)[\ell : k]$, es decir, $dr = sf$, lo cual equivale a $d = \frac{sf}{r} = \frac{r}{(r,f)} \frac{f}{r} = \frac{f}{(r,f)}$ y $h = \frac{f}{d} = (r, f)$. En resumen, tenemos:

Teorema 9.1.4. *Si \mathfrak{p} es un lugar de K , $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ son los lugares de $L = K\ell$ sobre \mathfrak{p} y $[\ell : k] = f$, entonces*

- (1) $d_{L/K}(\mathfrak{P}_i | \mathfrak{p}) = \frac{f}{(d_K(\mathfrak{p}), f)},$
- (2) $h = (d_K(\mathfrak{p}), f),$
- (3) $d_L(\mathfrak{P}_i) = \frac{d_K(\mathfrak{p})}{(d_K(\mathfrak{p}), f)}.$

\square

9.2. Campos ciclotómicos

Un campo ciclotómico numérico es de la forma $\mathbb{Q}(\zeta_n)$, $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$ y $\zeta_n^n = 1$. Ahora bien, el Teorema de Kronecker–Weber dice que toda extensión abeliana de \mathbb{Q} está contenida en una extensión ciclotómica. Equivalentemente, se tiene que si \mathbb{Q}^{ab} es la máxima extensión abeliana de \mathbb{Q} , entonces $\mathbb{Q}^{\text{ab}} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$. Notemos que ζ_n es un elemento de torsión de \mathbb{Z} actuando en $\overline{\mathbb{Q}}^* = \overline{\mathbb{Q}} \setminus \{0\}$, por exponenciación donde $\overline{\mathbb{Q}}$ es una cerradura algebraica de \mathbb{Q} . Esto es, si $\alpha \in \overline{\mathbb{Q}}^*$ y $n \in \mathbb{Z}$, la acción está definida por: $n \circ \alpha := \alpha^n$. Entonces

$$\begin{aligned} \mathbb{Q}^{\text{ab}} &= \mathbb{Q}(\text{tor } \overline{\mathbb{Q}}^*), \quad \text{donde} \\ \text{tor } \overline{\mathbb{Q}}^* &= \text{torsión de } \overline{\mathbb{Q}}^* = \{\alpha \in \overline{\mathbb{Q}}^* \mid \text{existe } n \in \mathbb{N} \text{ con } \alpha^n = 1\}. \end{aligned}$$

Pretendemos hacer un análogo a todo lo anterior para campos de funciones congruentes.

Sea $k = \mathbb{F}_q$ y K un campo de funciones racionales sobre k : $K = \mathbb{F}_q(T)$. Sea $R_T := \mathbb{F}_q[T]$ el anillo de polinomios sobre \mathbb{F}_q . Se tiene que K es el campo de cocientes de R_T .

Sea \overline{K} una cerradura algebraica de K y A el anillo de endomorfismos de \overline{K} sobre \mathbb{F}_q :

$$\begin{aligned} A = \text{End}_{\mathbb{F}_q}(\overline{K}) &= \{\varphi: \overline{K} \rightarrow \overline{K} \mid \varphi(a+b) = \varphi(a) + \varphi(b), \\ &\quad \varphi(\alpha a) = \alpha \varphi(a) \ \forall \alpha \in \mathbb{F}_q, \ \forall a, b \in \overline{K}\}. \end{aligned}$$

Entonces A es un anillo y un \mathbb{F}_q -módulo, es decir, en este caso, \mathbb{F}_q -espacio vectorial, donde la multiplicación de A es la composición. El anillo A tiene dos elementos sobresalientes:

Definición 9.2.1.

- (i) Sea φ el automorfismo de Frobenius de \overline{K} sobre \mathbb{F}_q , es decir, $\varphi: \overline{K} \rightarrow \overline{K}$, $u \mapsto u^q$.
- (ii) Sea μ_T la multiplicación por T : $\mu_T: \overline{K} \rightarrow \overline{K}$, $u \mapsto Tu$.

Sea $\xi: R_T \rightarrow A$ la substitución de T por $\varphi + \mu_T$, es decir, si $f(T) \in R_T$ es un polinomio, $\xi(f(T)) = f(\varphi + \mu_T) \in A$ es el endomorfismo dado por: si $f(T) = a_d T^d + \dots + a_1 T + a_0$, $f(\varphi + \mu_T)(u) = a_d((\varphi + \mu_T)^d(u) + \dots + a_1(\varphi + \mu_T)(u) + a_0 u$ para $u \in \overline{K}$. Es decir $\xi: R_T \rightarrow A$ está dado por $\xi(T) = \varphi + \mu_T$.

Entonces ξ es un homomorfismo de anillos y bajo ξ , \overline{K} es un R_T -módulo, lo cual es el análogo a que $\overline{\mathbb{Q}}^*$ es un \mathbb{Z} -módulo.

Notemos que para $u \in \overline{K}$,

$$\begin{aligned} (\varphi \circ \mu_T)(u) &= \varphi(Tu) = T^q u^q, \\ (\mu_T^q \circ \varphi)(u) &= \mu_T^q(u^q) = T^q u^q \end{aligned}$$

es decir, $\varphi \circ \mu_T = \mu_T^q \circ \varphi$ y en particular $\varphi \circ \mu_T \neq \mu_T \circ \varphi$.

Con el fin de hacer la analogía con $\overline{\mathbb{Q}}^*$ y \mathbb{Z} hacemos la siguiente notación:

Notación 9.2.2. Si $u \in \overline{K}$ y $M \in R_T$ denotamos $u^M = M(\varphi + \mu_T)(u)$. Esto es, $u^M = M \circ u = \xi(M)(u) = M(\varphi + \mu_T)(u)$.

Se tiene que para $u \in \overline{K}$, $M, N \in R_T$, entonces

$$u^{M+N} = u^M + u^N \quad \text{y} \quad (u^M)^N = u^{MN} = u^{NM} = (u^N)^M.$$

Teorema 9.2.3. Sea $M = a_d T^d + \cdots + a_1 T + a_0$ con $a_d \neq 0$. Entonces $u^M = \sum_{i=0}^d \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$ donde $\begin{bmatrix} M \\ i \end{bmatrix}$ es un polinomio de R_T de grado $(d-i)q^i$ y $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$, $\begin{bmatrix} M \\ d \end{bmatrix} = a_d$.

Demostración. Se tiene $u^T = (\varphi + \mu_T)(u) = u^q + Tu$. Vamos a probar por inducción en el grado de M que $u^M = \sum_{i=0}^d \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$ para algunos $\begin{bmatrix} M \\ i \end{bmatrix} \in R_T$, es decir, $\text{gr}_u u^M = q^{\text{gr}_T M}$. Esto se cumple para $d=0$ y $d=1$ donde $d = \text{gr}_T M$. Se tiene

$$\begin{aligned} u^{T^{i+1}} &= (u^{T^i})^T = T(u^{T^i}) = T\left(\sum_{j=0}^i \begin{bmatrix} T^i \\ j \end{bmatrix} u^{q^j}\right) \\ &= (\varphi + \mu_T)\left(\sum_{j=0}^i \begin{bmatrix} T^i \\ j \end{bmatrix} u^{q^j}\right) = \sum_{j=0}^i \begin{bmatrix} T^i \\ j \end{bmatrix}^q u^{q^{j+1}} + \sum_{j=0}^i T \begin{bmatrix} T^i \\ j \end{bmatrix} u^{q^j} \end{aligned} \quad (9.1)$$

de donde se sigue lo afirmado. Más aún, de la expresión anterior se obtiene

$$u^{T^{i+1}} = \sum_{j=0}^{i+1} \begin{bmatrix} T^{i+1} \\ j \end{bmatrix} u^{q^j} = \sum_{j=1}^{i+1} \begin{bmatrix} T^i \\ j-1 \end{bmatrix} u^{q^j} + \sum_{j=0}^i T \begin{bmatrix} T^i \\ j \end{bmatrix} u^{q^j}$$

por lo que

$$\begin{bmatrix} T^{i+1} \\ j \end{bmatrix} = \begin{bmatrix} T^i \\ j-1 \end{bmatrix}^q + T \begin{bmatrix} T^i \\ j \end{bmatrix}, \quad 0 \leq j \leq i+1 \quad (9.2)$$

donde definimos $\begin{bmatrix} T^i \\ \ell \end{bmatrix} = 0$ si $\ell < 0$ o $\ell > i$.

Por lo lado tenemos que si $M, N \in R_T$, $\text{gr}_T M, \text{gr}_T N \leq d$, $\alpha, \beta \in \mathbb{F}_q$, entonces

$$\begin{aligned} u^{\alpha M + \beta N} &= \sum_{i=0}^d \begin{bmatrix} \alpha M + \beta N \\ i \end{bmatrix} u^{q^i} = \alpha u^M + \beta u^N \\ &= \alpha \sum_{i=0}^d \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i} + \beta \sum_{i=0}^d \begin{bmatrix} N \\ i \end{bmatrix} u^{q^i} \end{aligned}$$

de donde

$$\begin{bmatrix} \alpha M + \beta N \\ i \end{bmatrix} = \alpha \begin{bmatrix} M \\ i \end{bmatrix} + \beta \begin{bmatrix} N \\ i \end{bmatrix}. \quad (9.3)$$

En particular, si $M = a_d T^d + \cdots + a_0$, entonces

$$\begin{bmatrix} M \\ i \end{bmatrix} = \sum_{j=0}^d a_j \begin{bmatrix} T^j \\ i \end{bmatrix}.$$

Ahora $\begin{bmatrix} T^0 \\ i \end{bmatrix} = \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{cases} 1 & \text{si } i = 0 \\ 0 & \text{si } i > 0 \end{cases}$ de donde $\text{gr}_T \begin{bmatrix} T^0 \\ 1 \end{bmatrix} = 0$ y $\begin{bmatrix} T^{j+1} \\ i \end{bmatrix} = \begin{bmatrix} T^j \\ i-1 \end{bmatrix}^q + T \begin{bmatrix} T^j \\ i \end{bmatrix}.$

Por inducción en j , suponemos $\text{gr}_T \begin{bmatrix} T^j \\ i \end{bmatrix} = (j-i)q^i$, $0 \leq i \leq j$, entonces

$$\begin{aligned} \text{gr}_T \begin{bmatrix} T^j \\ i-1 \end{bmatrix}^q &= (j-(i-1))q^{i-1}q = (j-i+1)q^i, \\ \text{gr}_T \begin{bmatrix} T^j \\ i \end{bmatrix} &= (j-i)q^i \end{aligned}$$

y por tanto, de (9.2) se tiene $\text{gr}_T \begin{bmatrix} T^{i+1} \\ i \end{bmatrix} (j-i+1)q^i = (j+1-i)q^i$ de donde obtenemos el resultado para $M = T^j$. El caso general se sigue de (9.3).

Similarmente, por inducción en i suponemos $\begin{bmatrix} T^i \\ 0 \end{bmatrix} = T^i$, entonces de (9.2) se tiene $\begin{bmatrix} T^{i+1} \\ 0 \end{bmatrix} = \begin{bmatrix} T^i \\ -1 \end{bmatrix}^q + T \begin{bmatrix} T^i \\ 0 \end{bmatrix} = T^{i+1}.$

Ahora

$$\begin{bmatrix} M \\ 0 \end{bmatrix} = \sum_{i=0}^d a_i \begin{bmatrix} T^i \\ 0 \end{bmatrix} = \sum_{i=0}^d a_i T^i = M \quad \text{y} \quad \begin{bmatrix} M \\ d \end{bmatrix} = \sum_{i=0}^d a_i \begin{bmatrix} T^i \\ d \end{bmatrix} = a_d \begin{bmatrix} T^d \\ d \end{bmatrix} = a_d. \quad \square$$

Resulta ser que la acción de R_T sobre \overline{K} : $M \circ u := u^M$ es la análoga a la acción de \mathbb{Z} sobre $\overline{\mathbb{Q}}^*$: $n \circ \xi := \xi^n$. El campo ciclotómico numérico corresponde a

$$\{\xi \in \overline{\mathbb{Q}}^* \mid \xi^n = 1\} = \{\zeta_n^a\}_{a=0}^{n-1},$$

donde $\zeta_n = \exp(2\pi i/n)$.

Por analogía, el campo de funciones ciclotómico debe corresponder a $\{u \in \overline{K} \mid u^M = 0\}.$

Definición 9.2.4. Sea Λ_M los elementos de \overline{K} que corresponden a la M -torsión de la acción de R_T , es decir,

$$\Lambda_M = \{u \in \overline{K} \mid u^M = 0\}.$$

Λ_M recibe el nombre del *módulo de Carlitz-Hayes* de M .

Proposición 9.2.5. *Se tiene que Λ_M es un R_T -submódulo de \overline{K} .*

Demostración. Si $u \in \Lambda_M$ y $N \in R_T$, entonces $(u^N)^M = u^{NM} = u^{MN} = (u^M)^N = 0^N = 0$, por lo que $u^N \in \Lambda_M$. \square

Observación 9.2.6. Si $\alpha \in \mathbb{F}_q^*$, $\Lambda_{\alpha M} = \Lambda_M$ pues $u^{\alpha M} = (u^\alpha)^M = (\alpha u)^M = \alpha u^M = 0 \iff u^M = 0$.

Debido a esto, siempre podemos considerar, sin pérdida de generalidad, polinomios mónicos.

Los siguientes resultados nos muestran que Λ_M es el equivalente a $W_n = \{\xi \in \mathbb{C} \mid \xi^n = 1\} \cong C_n \cong \mathbb{Z}/n\mathbb{Z}$ el grupo cíclico de n elementos. En nuestro caso, para ser análogo, necesitamos que Λ_M sea un R_T -módulo cíclico isomorfo a R_T/M , es decir, nuevamente R_T es substituto de \mathbb{Z} y M de n .

Proposición 9.2.7. *Se tiene que u^M es un polinomio separable en u de grado q^d , donde $M \in R_T$ es de grado d , de donde Λ_M es un conjunto finito de q^d elementos. Más aún, Λ_M es un \mathbb{F}_q -espacio vectorial de dimensión d .*

Demostración. Sea $M = a_d T^d + \cdots + a_1 T + a_0$. Entonces

$$u^M = \sum_{i=0}^d \binom{M}{i} u^{q^i}, \quad (u^M)' = \frac{d}{du}(u^M) = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0.$$

Así, $(u^M)'$ no tiene raíces y u^M es separable en u . Además $\text{gr}_u u^M = q^d$, por lo que $|\Lambda_M| = q^d$. Claramente Λ_M es un \mathbb{F}_q -espacio vectorial y por tanto de dimensión d . \square

Para continuar analizando la analogía entre W_n y Λ_M , notemos que si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la descomposición en primos, $W_n \cong \prod_{i=1}^r W_{p_i^{\alpha_i}}$. El análogo para Λ_M es:

Proposición 9.2.8. *Si $M = \prod_{i=1}^r P_i^{\alpha_i}$ es la descomposición de M como producto de irreducibles, entonces*

$$\Lambda_M \cong \prod_{i=1}^r \Lambda_{p_i^{\alpha_i}}$$

como R_T -módulos.

Demostración. No es más que un resultado general de módulos sobre dominios de ideales principales. \square

Para probar que Λ_M es R_T -cíclico, el paso esencial es cuando $M = P^n$, P irreducible.

Proposición 9.2.9. *Si $M = P^n$, entonces $\Lambda_{P^n} \cong R_T/P^n$ como R_T -módulos y por lo tanto Λ_{P^n} es R_T -cíclico.*

Demostración. Lo hacemos por inducción en n . Para $n = 1$, sea $\xi \in \Lambda_P \setminus \{0\}$ y sea $\theta: R_T \rightarrow \Lambda_P$ dada por $N \mapsto \xi^N$. Entonces $P \in \text{núc } \theta$ y $\langle P \rangle$ es maximal. Puesto que $\theta(1) = \xi \neq 0$, se sigue que $\text{núc } \theta = \langle P \rangle$ y $R_T/\langle P \rangle$ es submódulo de Λ_M . Puesto que $|R_T/\langle P \rangle| = |\Lambda_P| = q^d$ donde $d = \text{gr } P$, se sigue que $R_T/\langle P \rangle \cong \Lambda_P$ y cualquier $\xi \in \Lambda_P \setminus \{0\}$ es generador.

Supongamos que Λ_{P^n} es cíclico con generador λ . Sea $\mu: \Lambda_{P^{n+1}} \rightarrow \Lambda_{P^n}$ dada por $\xi \mapsto \xi^P$. Se tiene que $\text{núc } \mu = \Lambda_P$ y $|\Lambda_{P^{n+1}}/\Lambda_P| = |\Lambda_{P^n}| = q^{nd}$ por lo que $\Lambda_{P^{n+1}}/\Lambda_P \cong \Lambda_{P^n}$, es decir $0 \rightarrow \Lambda_P \rightarrow \Lambda_{P^{n+1}} \xrightarrow{\mu} \Lambda_{P^n} \rightarrow 0$ es R_T -exacta.

Sea $\xi \in \Lambda_{P^{n+1}}$ tal que $\mu(\xi) = \xi^P = \lambda$ genera Λ_{P^n} como R_T -módulos. Sea A el R_T -módulo generado por ξ , $A = R_T \circ \xi = \xi^{R_T}$. Se tiene que $A \subseteq \Lambda_{P^{n+1}}$ y $A \cong R_T/\text{an}(\xi)$ donde $\text{an}(\xi) := \{N \in R_T \mid \xi^N = 0\}$.

Ahora bien $P^{n-1} \notin \text{an}(\xi)$ pues $\lambda^{P^{n-1}} = \mu(\xi^{P^{n-1}}) \neq 0$. Sea $\alpha \in \Lambda_{P^{n+1}}$ cualquiera. Entonces $\mu(\alpha) = \alpha^P \in \Lambda_{P^n} = R_T \circ \lambda$. Por tanto existe $B \in R_T$ tal que $\alpha^P = \lambda^B = \mu(\xi^B) = \xi^{PB}$. Entonces $(\alpha - \xi^B)^P = 0$, es decir, $\alpha - \xi^B \in \Lambda_P = \text{núc } \mu$.

Se tiene que ξ^P genera Λ_{P^n} por lo que $(\xi^P)^{P^{n-1}} = \xi^{P^n} \neq 0$ y $\xi^{P^n} \in \Lambda_P$. Por el caso $n = 1$, ξ^{P^n} genera Λ_P . En particular, existe $C \in R_T$ tal que $\xi^{P^n C} = \alpha - \xi^B$ o $\xi^{B+P^n C} = \alpha$, es decir, ξ genera $\Lambda_{P^{n+1}}$ como R_T -módulo. Finalmente, $\langle P^{n+1} \rangle \subseteq \text{an}(\xi) \subsetneq \langle P^n \rangle$.

Sea $\text{an}(\xi) = \langle Q \rangle$. Entonces $P^n | Q$, $Q \neq P^n$, por lo que $Q = P^n Q_1 | P^{n+1}$, es decir, $Q_1 | P$ y Q_1 no es unidad. Se sigue que $Q_1 = P$, $Q = P^{n+1}$, $\text{an}(\xi) = \langle P^{n+1} \rangle$ y $\Lambda_{P^{n+1}} = R_T \circ \xi \cong R_T/\text{an}(\xi) = R_T/\langle P^{n+1} \rangle$. \square

Teorema 9.2.10. *Para todo $M \in R_T$, $M \neq 0$, Λ_M es un R_T -módulo cíclico y $\Lambda_M \cong R_T/\langle M \rangle$ como R_T -módulos.*

Demostración. Es inmediato de las Proposiciones 9.2.8 y 9.2.9. \square

Como en grupos, se tiene que:

Proposición 9.2.11. *Sean λ un generador de Λ_M y $A \in R_T$. Entonces λ^A es generador de Λ_M si y sólo si A y M son primos relativos.*

Demostración. Se tiene que λ^A genera a Λ_M si y sólo si $\lambda \in R_T \circ \lambda^A = \{\lambda^{AB} \mid B \in R_R\}$, es decir, si y sólo si existe $C \in R_T$ tal que $\lambda = \lambda^{AC}$ lo cual equivale a que $\lambda^{1-AC} = 0$. Puesto que $\text{an}(\lambda) = \langle M \rangle$, $\lambda^{1-AC} = 0$ si y sólo si $M | 1 - AC$. \square

Definición 9.2.12. Sea $M \in R_T \setminus \{0\}$ y sea Λ_M el módulo de Carlitz–Hayes de M . Se define el *campo de funciones ciclotómico determinado por M* al campo $K(\Lambda_M)$.

Teorema 9.2.13. Se tiene que si λ_M es un generador de Λ_M como R_T -módulo, entonces $K(\Lambda_M) = K(\lambda_M)$ y $K(\Lambda_M)/K$ es una extensión de Galois.

Demostración. Se tiene $\lambda_M^{R_T} = \Lambda_M = \{\lambda_M^A \mid A \in R_T\}$ por lo que $K(\Lambda_M) = K(\lambda_M)$ pues cada elemento $\xi \in \Lambda_M$ es de la forma

$$\xi = \lambda_M^A = A(\mu_T + \varphi)(\lambda_M) \in K(\lambda_M^q, \{T^s \lambda_M\}) = K(\lambda_M).$$

En particular, puesto que Λ_M es el conjunto de raíces del polinomio $u^M \in R_T[u] \subseteq K[u]$ y u^M es separable (Proposición 9.2.7), $K(\Lambda_M)/K$ es normal y separable, es decir, Galois. \square

Definición 9.2.14. Para $M \in R_T \setminus \{0\}$, G_M denota al grupo de Galois de $K(\Lambda_M)/K$: $G_M := \text{Gal}(K(\Lambda_M)/K)$.

En el caso numérico, tenemos que $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Por tanto, en el caso de campos de funciones podríamos esperar que $G_M \cong (R_T/\langle M \rangle)^*$ el grupo de unidades del anillo $R_T/\langle M \rangle$. Ahora bien, notemos que

$$(R_T/\langle M \rangle)^* = \{A \bmod M \mid (A, M) = 1\}$$

y que el número de generadores de Λ_M es precisamente $|(R_T/\langle M \rangle)^*|$ (Proposición 9.2.11). Ahora $|(\mathbb{Z}/n\mathbb{Z})^*|$ está dada por la función ϕ de Euler. Aquí tenemos el análogo.

Definición 9.2.15. Se define la función “Fi” de Euler por:

$$\Phi(M) := |(R_T/\langle M \rangle)^*|$$

para $M \in R_T \setminus \{0\}$.

Puesto que $\langle M \rangle = \langle \alpha M \rangle$ para $\alpha \in \mathbb{F}_q^*$, $\Phi(\alpha M) = \Phi(M)$ para $\alpha \in \mathbb{F}_q^*$.

Para el Teorema Chino del Residuo, tenemos que si M y N son primos relativos, entonces $R_T/\langle MN \rangle \cong R_T/\langle M \rangle \times R_T/\langle N \rangle$ y $(R_T/\langle MN \rangle)^* \cong (R_T/\langle M \rangle)^* \times (R_T/\langle N \rangle)^*$. En particular se tiene $\Phi(MN) = \Phi(M)\Phi(N)$ para M y N primos relativos.

Por otro lado, si P es irreducible, entonces $R_T/\langle P \rangle$ es el campo de q^d elementos donde $d = \text{gr } P$. Por tanto $|(R_T/\langle P \rangle)^*| = q^d - 1 = \Phi(P)$. Para $n \geq 2$, se tiene que si $(R_T/\langle P^n \rangle)^* \xrightarrow{\theta} (R_T/\langle P^{n-1} \rangle)^*$ es el mapeo natural, $\theta(A \bmod P^n) = A \bmod P^{n-1}$, entonces $\text{nuc } \theta = \{1 + P^{n-1}B \bmod P^n \mid B \in R_T\} \cong R_T/\langle P \rangle$. En particular

$$0 \longrightarrow R_T/\langle P \rangle \xrightarrow{\mu} (R_T/\langle P^n \rangle)^* \xrightarrow{\theta} (R_T/\langle P^{n-1} \rangle)^* \longrightarrow 1$$

es exacta, donde $\mu(B \bmod P) = 1 + P^{n-1}B \bmod P^n$.

De inmediato obtenemos dos resultados:

- (I) $\Phi(P^n) = \Phi(P^{n-1})|_{R_T/\langle P \rangle} = \Phi(P^{n-1})(q^d)$,
 (II) $R_T/\langle P \rangle \cong D_{P^n, P^{n-1}} = \{\bar{A} \in (R_T/\langle P^n \rangle)^* \mid A \equiv 1 \text{ mód } P^{n-1}\} = \text{núc } \theta$.

Si por inducción suponemos $\Phi(P^n) = q^{nd} - q^{(n-1)d}$, entonces $\Phi(P^{n+1}) = \Phi(P^n)q^d = (q^{nd} - q^{(n-1)d})q^d = q^{(n+1)d} - q^{nd}$.

De manera análoga, si

$$\pi: (R_T/\langle P^n \rangle)^* \longrightarrow (R_T/\langle P \rangle)^*$$

está dada por $\pi(A \text{ mód } P^n) = A \text{ mód } P$, se tiene

$$\text{núc } \pi = D_{P^n, P} = \{\bar{A} \in (R_T/\langle P^n \rangle)^* \mid A \equiv 1 \text{ mód } P\} \cong R_T/\langle P^{n-1} \rangle$$

y en general se tiene, para $1 \leq m < n$, que la sucesión

$$1 \longrightarrow D_{P^n, P^m} \longrightarrow (R_T/\langle P^n \rangle)^* \xrightarrow{\varphi} (R_T/\langle P^m \rangle)^* \longrightarrow 1$$

es exacta donde $\varphi(A \text{ mód } P^n) = A \text{ mód } P^m$, y

$$D_{P^n, P^m} = \{A \text{ mód } P^n \in (R_T/\langle P^n \rangle)^* \mid A \equiv 1 \text{ mód } P^m\} \cong R_T/\langle P^{n-m} \rangle.$$

El isomorfismo $D_{P^n, P^m} \cong R_T/\langle P^{n-m} \rangle$ está dado por $B \text{ mód } P^{n-m} \mapsto 1 + P^m B \text{ mód } P^n$. Resumiendo, tenemos:

Proposición 9.2.16. *La función Φ de Euler satisface:*

- (1) $\Phi(MN) = \Phi(M)\Phi(N)$ para M, N primos relativos.
- (2) $\Phi(P^n) = |R_T/\langle P^{n-1} \rangle| \Phi(P) = q^{nd} - q^{(n-1)d}$ donde P es irreducible, $n \geq 1$ y $d = \text{gr } P$.
- (3) Para $1 \leq m < n$ y P irreducible, la sucesión

$$0 \longrightarrow R_T/\langle P^{n-m} \rangle \longrightarrow (R_T/\langle P^n \rangle)^* \xrightarrow{\varphi} (R_T/\langle P^m \rangle)^* \longrightarrow 1$$

es exacta y $R_T/\langle P^{n-m} \rangle \cong D_{P^n, P^m}$.

(4) $\Phi(M)$ es el número de generadores de Λ_M . □

Proposición 9.2.17. *Sea $M \in R_T \setminus \{0\}$. Entonces $G_M \subseteq (R_T/\langle M \rangle)^*$.*

Demostración. Se tiene que si $\lambda = \lambda_M$ es un generador de Λ_M , entonces $K(\Lambda_M) = K(\lambda_M)$. Por tanto $\sigma \in G_M$ está determinado por su acción en λ y puesto que $\sigma\lambda$ es un conjugado de λ , $\sigma\lambda \in \Lambda_M$. Si $\sigma\lambda = \beta$, entonces $\lambda = \sigma^{-1}\beta$ por lo que necesariamente $\sigma\lambda$ es generador de Λ_M . Se sigue que $\sigma\lambda = \lambda^A$ para $\text{mcd}(A, M) = 1$. Denotemos σ por σ_A , es decir, $\sigma_A\lambda = \lambda^A$, $\text{mcd}(A, M) = 1$.

Sea $\varphi: G_M \rightarrow (R_T/\langle M \rangle)^*$, $\sigma_A \mapsto A \text{ mód } M$. Claramente φ es un monomorfismo de grupos. □

Corolario 9.2.18. Para $M \in R_T \setminus \{0\}$, $[K(\Lambda_M) : K] \leq \Phi(M)$. \square

Definición 9.2.19. Sea $S \in R_T$ un polinomio mónico. Definimos el *polinomio S -ciclotómico* por

$$\Psi_S(u) := \prod_{\substack{\text{mcd}(B,S)=1 \\ \text{gr } B < \text{gr } S}} (u - \lambda_S^B)$$

donde λ_S es un generador de Λ_S . Se tiene $\Psi_S(u) \in K(\Lambda_S)[u]$.

Notemos que $\Psi_S(u)$ es el análogo al polinomio ciclotómico usual

$$\psi_n(x) = \prod_{\substack{\text{mcd}(m,n)=1 \\ 0 \leq m \leq n}} (x - \zeta_n^m).$$

Resultó ser que $\psi_n(x) \in \mathbb{Q}[x]$ es irreducible de grado $\varphi(n) = (\mathbb{Z}/n\mathbb{Z})^*$. Veremos que $\psi_S(u) \in K[u]$ es irreducible de grado $\Phi(S)$. Ahora bien, $\text{gr}_u \Psi_S(u) = \Phi(S)$ por la Proposición 9.2.11.

Proposición 9.2.20. Se tiene que $\Psi_S(u) \in K[u]$.

Demostración. Sea $\sigma_A \in G_S$. Entonces $\sigma_A(\lambda_S) = \lambda_S^A$ y si $\text{mcd}(B, S) = 1$, $\sigma_A(\lambda_S^B) = \lambda_S^{BA}$ con $\text{mcd}(AB, S) = 1$. Por lo tanto

$$\sigma_A(\Psi_S(u)) = \prod_{\substack{\text{mcd}(B,S)=1 \\ \text{gr } B < \text{gr } S}} (u - \lambda_S^{AB}).$$

Tomando AB mód S y puesto que multiplicación por A es un automorfismo de $(R_T/\langle S \rangle)^*$, se sigue que $\sigma_A(\Psi_S(u)) = \Psi_S(u)$, $\sigma_A \in G_M$ de donde $\Psi_S(u) \in K[u]$. \square

Como en el caso numérico tenemos:

Proposición 9.2.21.

(1) Si $M, N \in R_T$ son polinomios mónicos con $M \neq N$, entonces $\text{mcd}(\Psi_M(u), \Psi_N(u)) = 1$.

(2) $u^M = \prod_{\substack{N|M \\ N \text{ mónico}}} \Psi_N(u)$, $M, N \in R_T$ mónicos.

(3) $\Psi_M(u) = \prod_{\substack{N|M \\ N \text{ mónico}}} (u^N)^{\mu(M/N)}$ donde

$$\mu(D) = \begin{cases} 1 & \text{si } D = 1, \\ (-1)^s & \text{si } D = P_1 \cdots P_s \text{ con } P_1, \dots, P_s \text{ mónicos e} \\ & \text{irreducibles distintos} \\ 0 & \text{en otro caso} \end{cases}$$

y M mónico.

Demostración.

- (1) Sea $D := \text{mcd}(\Psi_M(u), \Psi_N(u))$. Si $D \neq 1$, sea $\lambda \in \overline{K}$ raíz de D . Por tanto λ es raíz de $\Psi_M(u)$ y $\Psi_N(u)$, es decir, $\lambda = \lambda_M^A = \lambda_N^B$ para $\text{mcd}(A, M) = 1$, $\text{mcd}(B, N) = 1$ con $\text{gr } A < \text{gr } M$ y $\text{gr } B < \text{gr } N$. Por tanto se tiene $\lambda = \lambda_{MN}^{AN} = \lambda_{NM}^{BM}$ lo cual implica que $AN = BM$. Puesto que B y N son primos relativos lo mismo que A y M , se sigue que $B|A$ y $A|B$ con lo que se concluye que $A = B$ y por tanto $M = N$ lo cual es contrario a lo supuesto.
- Por tanto $D = \text{mcd}(\Psi_M(u), \Psi_N(u)) = 1$.
- (2) Claramente, si $N|M$, entonces $\Psi_N(u)|u^M$ y como para $N_1 \neq N_2$, $\text{mcd}(\Psi_{N_1}(u), \Psi_{N_2}(u)) = 1$, se sigue que $\prod_{\substack{N|M \\ N \text{ mónico}}} \Psi_N(u)|u^M$.

$$\text{Ahora } \text{gr} \left(\prod_{\substack{N|M \\ N \text{ mónico}}} \Psi_N(u) \right) = \sum_{\substack{N|M \\ N \text{ mónico}}} \Phi(N).$$

Si $M = P^n$ con P irreducible y $\text{gr } P = d$, se tiene

$$\begin{aligned} \sum_{N|M} \Phi(N) &= \sum_{i=0}^n \Phi(P^i) = \sum_{i=1}^n (q^{id} - q^{(i-1)d}) + 1 \\ &= q^{nd} - 1 + 1 = q^{nd} = q^{\text{gr } P^n}. \end{aligned}$$

En general si $M = P_1^{\alpha_1} \dots P_r^{\alpha_r}$

$$\begin{aligned} \sum_{\substack{N|M \\ N \text{ mónico}}} \Phi(N) &= \sum_{\substack{\beta_i=0 \\ i=1, \dots, r}} \Phi(P_1^{\beta_1} \dots P_r^{\beta_r}) = \prod_{i=1}^r \sum_{\beta_i=0}^{\alpha_i} \Phi(P_i^{\beta_i}) \\ &= \prod_{i=1}^r q^{\text{gr } P_i^{\beta_i}} = q^{\text{gr } M}. \end{aligned}$$

Por lo tanto $\text{gr} \left(\prod_{\substack{N|M \\ N \text{ mónico}}} \Psi_N(u) \right) = q^{\text{gr } M} = \text{gr } u^M$, lo cual implica $u^M = \prod_{N|M} \Psi_N(u)$.

- (3) La demostración es totalmente análoga a la del Corolario 3.2.15 (2). \square

Ahora veamos que la ramificación en campos de funciones es totalmente paralela a la de los campos ciclotómicos numéricos.

Definición 9.2.22. Al polo \mathfrak{p}_∞ de T en K lo llamamos *primo infinito*.

Proposición 9.2.23. Sean $P \in R_T$ mónico e irreducible de grado d y $M = P^n$, $n \in \mathbb{N}$. Entonces

- (I) Si \mathfrak{q} es cualquier otro divisor primo distinto a \mathfrak{p}_∞ y \mathfrak{p} , donde \mathfrak{p} es el primo asociado a P , entonces \mathfrak{q} no es ramificado.
 (II) El índice de ramificación de \mathfrak{p} en $K(\Lambda_M)/K$ es

$$e(\mathfrak{p}) = \Phi(M) = q^{dn} - q^{d(n-1)} = [K(\Lambda_M) : K].$$

Demostración.

Sea \mathcal{O}_M la cerradura entera de R_T en $K(\Lambda_M)$. Puesto que R_T es un dominio Dedekind, \mathcal{O}_M también lo es. Se tiene que los primos K ramificados en $K(\Lambda_M)/K$, diferente a \mathfrak{p}_∞ , son aquellos que aparecen en el discriminante $\mathfrak{d}_{\mathcal{O}_M/R_T}$. Sea λ generador de Λ_M . Entonces $R_T[\lambda] \subseteq \mathcal{O}_M$. Sean $g(u) := \text{Irr}(\lambda, u, K) \in K[u]$ y $f(u) := u^M$. Puesto que $f(\lambda) = 0$, existe $h(u) \in K[u]$ tal que $f(u) = h(u)g(u)$. Por tanto

$$M = f'(u) = h'(u)g(u) + h(u)g'(u)$$

de donde

$$M = f'(\lambda) = h'(\lambda)g(\lambda) + h(\lambda)g'(\lambda) = h(\lambda)g'(\lambda).$$

En particular $(g'(\lambda))_{\mathcal{O}_M} | (M)_{\mathcal{O}_M} = P^n \mathcal{O}_M$. Se tiene (Teorema 8.5.6)

$$\mathfrak{d}_{\mathcal{O}_M/R_T} = \langle F'(\alpha) \mid \alpha \in \mathcal{O}_M, K(\Lambda_M) = K(\alpha), F(u) = \text{Irr}(\alpha, u, K) \rangle.$$

En particular

$$\mathfrak{d}_{\mathcal{O}_M/R_T} | (g'(\lambda))_{K(\Lambda_M)} = P^n = (\mathfrak{p}_1 \cdots \mathfrak{p}_h)^{en} \quad \text{donde} \quad P\mathcal{O}_M = \langle \mathfrak{p}_1 \cdots \mathfrak{p}_h \rangle^e. \quad (9.4)$$

Por tanto los únicos posibles primos ramificados en $K(\Lambda_M)/K$ son \mathfrak{p} y \mathfrak{p}_∞ . Ahora

$$\begin{aligned} u^{P^n} &= (u^{P^{n-1}})^P = \sum_{i=0}^d \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i} \\ &= u^{P^{n-1}} \left(\sum_{i=0}^d \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1} \right) = u^{P^{n-1}} t(u) \end{aligned}$$

$$\text{con } t(u) = \frac{u^{P^n}}{u^{P^{n-1}}} = \sum_{i=0}^d \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1}.$$

Se tiene $t(\alpha) = 0 \iff \alpha \in \Lambda_{P^n} \setminus \Lambda_{P^{n-1}} \iff \alpha$ es generador de Λ_{P^n} . Por tanto $t(u) = \Psi_{P^n}(u)$ y

$$\begin{aligned}
t(u) &= \prod_{\gcd(A,M)=1} (u - \lambda^A) = \begin{bmatrix} P \\ 0 \end{bmatrix} + \sum_{i=1}^d \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i-1} \\
&= P + \sum_{i=1}^d \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i-1}.
\end{aligned}$$

Con $u = 0$, se tiene

$$t(0) = \pm \prod_{\gcd(A,M)=1} \lambda^A = P. \quad (9.5)$$

Ahora bien $u^A = um_A(u)$ con $m_A(u) \in R_T(u)$. En particular $\lambda^A = \lambda F(\lambda)$ y $\lambda | \lambda^A$. Para $(A, M) = 1$, λ^A es generador y por simetría se sigue que $\lambda^A | \lambda$, es decir $\lambda = \beta_A \lambda^A$ con $\beta_A \in \mathcal{O}_M^*$. Se sigue de (9.5) que $\pm P = \beta_0 \lambda^{\Phi(M)}$ para $\beta_0 \in \mathcal{O}_M^*$. De (9.4) obtenemos $\langle P \rangle_{\mathcal{O}_M} = \langle \mathfrak{p}_1 \cdots \mathfrak{p}_h \rangle^e = (\lambda)^{\Phi(M)}$ y en particular $v_{\mathfrak{p}_i}(\lambda) \geq 1$. Entonces $e = v_{\mathfrak{p}_i}((\mathfrak{p}_1 \cdots \mathfrak{p}_h)^e) = v_{\mathfrak{p}_i}(\lambda^{\Phi(M)}) \geq \Phi(M)$, esto es,

$$e \geq \Phi(M) = |(R_T / \langle M \rangle)^*| \geq [K(\Lambda_M) : K] \geq e$$

de donde $e = \Phi(M) = \Phi(P^n) = [K(\Lambda_{P^n}) : K] = q^{dn} - q^{d(n-1)}$. \square

Observación 9.2.24. De paso hemos obtenido que el polinomio ciclotómico $\Psi_{P^n}(u)$ satisface

$$\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}} = \frac{\prod_{N|P^n} \Psi_N(u)}{\prod_{N|P^{n-1}} \Psi_N(u)} = \prod_{\gcd(A,M)=1} (u - \lambda^A).$$

El caso general es consecuencia de la Proposición 9.2.23.

Teorema 9.2.25. Si $M \in R_T \setminus \{0\}$ un polinomio mónico. Entonces

- (1) $t(u) = \text{Irr}(\lambda, u, K) = \Psi_M(u)$ donde λ es generador de Λ_M . En particular $\Psi_M(u)$ es irreducible.
- (2) $G_M = \text{Gal}(K(\Lambda_M)/K) \cong (R_T / \langle M \rangle)^*$.
- (3) $[K(\Lambda_M) : K] = \Phi(M)$.
- (4) $M = P^n$ donde P es irreducible, entonces \mathfrak{p} es totalmente ramificado en $K(\Lambda_{P^n})/K$ donde $\langle P \rangle_K = \frac{\mathfrak{p}}{\mathfrak{p}_{\infty}^{\text{gt } P}}$.

Demostración. Si $M = P^n$, por la Proposición 9.2.23, se tiene

$$[K(\Lambda_{P^n}) : K] = \Phi(P^n) = |(R_T / \langle P^n \rangle)^*| = |G_{P^n}|.$$

Por otro lado, por la Proposición 9.2.17, se tiene $G_{P^n} \subseteq (R_T / \langle P^n \rangle)^*$. Por tanto $G_{P^n} \cong (R_T / \langle P^n \rangle)^*$ y P es totalmente ramificado pues $e = \Phi(P^n) = [K(\Lambda_{P^n}) : K]$. Esto es (4).

En general, si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ con P_1, \dots, P_r polinomios irreducibles distintos, $\Lambda_M \cong \bigoplus_{i=1}^r \Lambda_{P_i^{\alpha_i}}$. Si probamos que $[K(\Lambda_M) : K] = \Phi(M)$ entonces, puesto que $G_M \subseteq (R_T / \langle P^n \rangle)^*$, se seguirá la igualdad y también (2) y (3). Finalmente (1) se seguirá del hecho de que $t(\lambda) = 0$, $\text{gr}_u t(u) = \Phi(\Psi_M(u)) = \text{gr Irr}(\lambda, u, K)$ y de que $\text{Irr}(\lambda, u, K) | t(u)$.

En resumen, solo falta probar que $\Phi(M) = [K(\Lambda_M) : K]$. Ahora bien, puesto que \mathfrak{p}_i es totalmente ramificado en $K(\Lambda_{P_i^{\alpha_i}})/K$ y no ramificado en $\prod_{j \neq i} K(\Lambda_{P_j^{\alpha_j}})/K$, se sigue que

$$[K(\Lambda_M) : K] = \prod_{i=1}^r [K(\Lambda_{P_i^{\alpha_i}}) : K] = \prod_{i=1}^r \Phi(P_i^{\alpha_i}) = \Phi(M). \quad \square$$

Corolario 9.2.26. *El campo de constantes de $K(\Lambda_M)$ es \mathbb{F}_q y $K(\Lambda_M)/K$ es una extensión geométrica.*

Demostración. Sea $E_i := K(\Lambda_M / P_i^{\alpha_i})$, $1 \leq i \leq r$ donde $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$. Se tiene que $\text{Gal}(K(\Lambda_M)/E_i) \cong \text{Gal}(K(\Lambda_{P_i^{\alpha_i}})/K)$. Sea L la máxima extensión no ramificada de K contenida en $K(\Lambda_M)$. Ahora bien, $K(\Lambda_M)/E_i$ es totalmente ramificada en los primos que están sobre \mathfrak{p}_i y $E_i L/E_i$ es no ramificada. por lo que $E_i L = E_i$. Entonces $L \subseteq E_i$ para $1 \leq i \leq r$.

Se sigue que $K \subseteq L \subseteq \bigcap_{i=1}^r E_i = K$. En particular $L = K$ y cada extensión $K \subsetneq F \subseteq K(\Lambda_M)$ es ramificada. Sea \mathbb{F}_{q^s} el campo de constantes de $K(\Lambda_M)$. Entonces

$$K = \mathbb{F}_q(T) \subseteq \mathbb{F}_{q^s}(T) \subseteq K(\Lambda_M).$$

Se tiene que $\mathbb{F}_{q^s}(T)/\mathbb{F}_q(T)$ es no ramificada (Teorema 9.1.3). Por tanto $\mathbb{F}_{q^s}(T) = \mathbb{F}_q(T)$ y $\mathbb{F}_{q^s} = \mathbb{F}_q$, es decir, $s = 1$. \square

La ramificación del primo infinito \mathfrak{p}_∞ está dada por el siguiente resultado, el cual no probaremos.

Teorema 9.2.27. *Sea $M \in R_T \setminus \{0\}$. Entonces \mathfrak{p}_∞ es moderadamente ramificado en $K(\Lambda_M)/K$. Además se tiene $e_\infty = q - 1$, $f_\infty = 1$ y hay $h_\infty = \Phi(M)/(q - 1)$ divisores primos en $K(\Lambda_M)$ sobre \mathfrak{p}_∞ .* \square

Observación 9.2.28. Notemos que $K(\Lambda_M) = K$ si y solamente si $q = 2$ y $M = T$, $M = T + 1$ o $M = T(T + 1)$. Es decir, $\mathbb{F}_2(T)(\Lambda_T)$, $\mathbb{F}_2(T)(\Lambda_{T+1})$ y $\mathbb{F}_2(T)(\Lambda_{T(T+1)})$ juegan el papel de $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ en el caso de los campos numéricos. Debemos tener en cuenta siempre esta excepción para todo el desarrollo de los campos de funciones ciclotómicas.

En particular, para $q = 2$, \mathfrak{p}_∞ no es ramificado en ningún $K(\Lambda_M)/K$ y $K(\Lambda_{MT}) = K(\Lambda_M)$ para todo $M \in R_T$ con $T \nmid M$. Similarmente $K(\Lambda_{M(T+1)}) = K(\Lambda_M)$ para todo $M \in R_T$ tal que $(T + 1) \nmid M$.

9.3. Ramificación en $K(\Lambda_M)/K$

Aquí estamos considerando $K(\Lambda_M)/K$ donde $M \in R_T \setminus \{0\}$ es un polinomio mónico.

Proposición 9.3.1. *Se tiene que los primos ramificados en $K(\Lambda_M)/K$ son \mathfrak{p}_∞ y los divisores de M .*

Demostración. Se sigue de que $K(\Lambda_M) = \prod_{P|M} K(\Lambda_{P^\alpha})$, la Proposición 9.2.23 y el Teorema 9.2.27. \square

Dado un lugar \mathfrak{p} en K y $\mathfrak{P} \in K(\Lambda_M)$ sobre \mathfrak{p} , si D e I son los grupos de descomposición e inercia, entonces $\text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \cong D/I$ (ver después de la Definición 8.4.6). Si \mathfrak{p} es no ramificado, $I = \{1\}$ y $D \cong \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Puesto que $k(\mathfrak{P})$ y $k(\mathfrak{p})$ son campos finitos, $\text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ es un grupo cíclico generado por el automorfismo de Frobenius:

$$\sigma_{\mathfrak{p}}: k(\mathfrak{P}) \longrightarrow k(\mathfrak{P}), \quad \sigma_{\mathfrak{p}}(x) = x^{|k(\mathfrak{p})|} = x^{N(\mathfrak{p})}$$

donde denotamos $N(\mathfrak{p}) = |k(\mathfrak{p})| = |\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}|$. Así tenemos:

Proposición 9.3.2. *El automorfismo de Frobenius, el cual será denotado por $\left[\frac{K(\Lambda_M)/K}{\mathfrak{P}}\right]$, está caracterizado por la propiedad*

$$\left[\frac{K(\Lambda_M)/K}{\mathfrak{P}}\right](x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \quad \forall x \in \mathcal{O}_{\mathfrak{P}}. \quad \square$$

Como $K(\Lambda_M)/K$ es abeliana, $\left[\frac{K(\Lambda_M)/K}{\mathfrak{P}}\right]$ es independiente de \mathfrak{P} y sólo depende de \mathfrak{p} y lo denotamos $\left(\frac{K(\Lambda_M)/K}{P}\right)$ y se llama el *símbolo de Artin*.

Teorema 9.3.3. *Sea P un polinomio irreducible que no divide a M . Entonces el mapeo:*

$$\begin{aligned} \varphi_P: \Lambda_M &\longrightarrow \Lambda_M \\ \lambda &\longmapsto \lambda^P \end{aligned}$$

corresponde al símbolo de Artin $\left(\frac{K(\Lambda_M)/K}{P}\right)$.

Demostración. Sea $(R_T)_P = \left\{\frac{f}{g} \mid f, g \in R_T, P \nmid g\right\}$ y sea $(P)_K := \frac{\mathfrak{p}}{\mathfrak{p}_{\infty}^{\text{gr } P}}$. Entonces $k(\mathfrak{p}) = (R_T)_P / P(R_T)_P \cong R_T / \langle P \rangle \cong \mathbb{F}_{q^d}$ donde $d = \text{gr } P$.

Sea \mathfrak{P} un lugar en $K(\Lambda_M)$ sobre \mathfrak{p} . Entonces $N(\mathfrak{p}) = |\mathbb{F}_{q^d}| = q^d$, $K(\Lambda_M) \subseteq \mathcal{O}_{\mathfrak{P}}$. Entonces

$$\left(\frac{K(\Lambda_M)/K}{P}\right)(\lambda) \equiv \lambda^{q^d} \pmod{\mathfrak{P}}.$$

Ahora $u^P = u\Psi_P(u) = u(u^{q^d-1} + \beta_{q^d-2}u^{q^d-2} + \cdots + \beta_1u + \beta_0)$. Puesto que $\Psi_P(u) = \prod_{\text{mcd}(A,P)=1} (u - \lambda^A)$, λ generador de Λ_P y $\Psi_P(0) = \pm \prod_{\text{mcd}(A,P)=1} \lambda^A = P$ por (9.5), se tiene que $P|\beta_i$, $0 \leq i \leq q^d - 2$, lo cual implica que $\lambda^P = \lambda^{q^d} \pmod{\mathfrak{P}}$.

De la expresión $u^M = \prod_{A \pmod M} (u - \lambda^A)$, tomando derivadas con respecto a u , se tiene que $M = \sum_{A \pmod M} \left(\prod_{\substack{B \not\equiv A \\ B \pmod M}} (u - \lambda^B) \right)$ que es constante en u . Sea $u = \lambda^C$. Entonces $M = \prod_{\substack{C \not\equiv B \\ B \pmod M}} (\lambda^C - \lambda^B)$ y puesto que $P \nmid M$ se sigue que $\lambda^C \not\equiv \lambda^B \pmod{\mathfrak{P}}$ para $C \not\equiv B \pmod M$. En particular $\lambda^P \equiv \lambda^Q \pmod{\mathfrak{P}}$ implica $\lambda^P = \lambda^Q$.

Finalmente $\lambda^P \equiv \left(\frac{K(\Lambda_M)/K}{P}\right)\lambda \equiv \lambda^{q^d} \pmod{\mathfrak{P}}$, de donde se sigue que $\varphi_P = \left(\frac{K(\Lambda_M)/K}{P}\right)$. \square

Con la notación usual de e_P = ramificación de P , f_P = grado de inercia y h_P = número de primos encima de P , tenemos:

Proposición 9.3.4. *Sea $M \in R_T \setminus \{0\}$ y sea P un polinomio irreducible que no divide a P . En $K(\Lambda_M)/K$ tenemos*

$$e_P = 1, \quad f_P = o(P \pmod M), \quad h_P = \Phi(M)/f_P.$$

Demostración. Sea λ generador de Λ_M , $K(\Lambda_M) = K(\lambda)$. Sea \mathfrak{P} un divisor primo en $K(\Lambda_M)$ dividiendo a \mathfrak{p} donde $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}^{\frac{P}{f_P}}}$. Entonces

$$\begin{aligned} \mathcal{O}_{\mathfrak{P}} &= \{\xi \in K(\Lambda_M) \mid v_{\mathfrak{P}}(\xi) \geq 0\} \quad \text{y} \\ f_P &= [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : (R_T)_P/P(R_T)_P] = [(\mathcal{O}_M)_{\mathfrak{P}}/\mathfrak{P}(\mathcal{O}_M)_{\mathfrak{P}} : R_T/\langle P \rangle] \\ &= [\mathcal{O}_M/\mathfrak{P}\mathcal{O}_M : R_T/\langle P \rangle] \end{aligned}$$

donde \mathcal{O}_M es la cerradura entera de R_T en $K(\Lambda_M)$.

Sea $d = \text{gr } P$. Puesto que $P \nmid M$, \mathfrak{p} no es ramificado en $K(\Lambda_M)/K$ y el símbolo de Artin $\varphi_P = \left(\frac{K(\Lambda_M)/K}{P}\right)$ en P está dado por $\varphi_P(\lambda) = \lambda^P$. Entonces $e_P = 1$ y $h_P = [K(\Lambda_M) : K]/f_P = \Phi(M)/f_P$.

Finalmente, f_P es el orden de φ_P , es decir f_P es el mínimo número natural tal que $\varphi_P^{f_P} = \text{Id} \in G_M = \text{Gal}(K(\Lambda_M)/K)$. Se tiene $\varphi_P^f = 1 \iff \varphi_P^f(\lambda) = \lambda^{P^f} = \lambda \iff \lambda^{P^f-1} = 0 \iff M|P^f - 1$.

Se sigue que $f_P = o(P \pmod M)$ es el mínimo número natural tal que $M|P^{f_P} - 1$. \square

El resultado general sobre ramificación está dado por:

Teorema 9.3.5. Sea $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \in R_T$ donde P_1, \dots, P_r son polinomios irreducibles y sea $K(\Lambda_M)/K$. Si $P \in R_T$ es distinto a P_1, \dots, P_r y \mathfrak{p}_∞ , entonces

$$e_P = 1, \quad f_P = o(P \bmod M) \quad y \quad h_P = \Phi(M)/f_P.$$

Si $P = P_i$ para algún $1 \leq i \leq r$, se tiene

$$e_P = \Phi(P_i^{\alpha_i}), \quad f_P = o(P_i \bmod (M/P_i^{\alpha_i})) \quad y$$

$$h_P = \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})f_{P_i}} = \frac{\Phi(M/P_i^{\alpha_i})}{o(P_i \bmod (M/P_i^{\alpha_i}))}.$$

Finalmente, para \mathfrak{p}_∞ se tiene:

$$e_\infty = q - 1, \quad f_\infty = 1 \quad y \quad h_\infty = \Phi(M)/(q - 1).$$

Demostración. El resultado se sigue de las Proposiciones 9.2.23, 9.3.4 y el Teorema 9.2.27. \square

También tenemos el resultado análogo al caso numérico que establece $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ (Teorema 3.2.30).

Proposición 9.3.6. Sea $M = P^n$, $P \in R_T$ irreducible. Entonces $\mathcal{O}_M = R_T[\lambda_M]$ donde \mathcal{O}_M es la cerradura entera de R_T en $K(\Lambda_M)$ y λ_M es un generador de Λ_M .

Demostración. Sea $\lambda = \lambda_M$. Se tiene $R_T[\lambda] \subseteq \mathcal{O}_M$. Ahora sea $\alpha \in \mathcal{O}_M$. Puesto que $\{1, \lambda, \dots, \lambda^{\Phi(M)-1}\}$ es base de $K(\Lambda_M)/K$, existen $a_0, a_1, \dots, a_r \in K$ tales que $\alpha = a_0 + a_1\lambda + \dots + a_r\lambda^r$ con $r = \Phi(M) - 1$. Para probar el resultado, queremos probar que $a_i \in R_T$ para $i = 0, 1, \dots, r$. En la demostración de la Proposición 9.2.23 se probó que $v_{\mathfrak{P}}(\lambda) = 1$ donde \mathfrak{P} es el único divisor en $K(\Lambda_M)$ sobre \mathfrak{p} , $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{gr_P}}$.

Se tiene que si $a_i \neq 0$, $v_{\mathfrak{P}}(a_i\lambda^i) = i + \Phi(P^n)v_{\mathfrak{P}}(a_i) \equiv i \bmod \Phi(M)$ y por tanto $i \neq j$, $a_i \neq 0 \neq a_j$, $v_{\mathfrak{P}}(a_i\lambda^i) \neq v_{\mathfrak{P}}(a_j\lambda^j)$. Por tanto

$$0 \leq v_{\mathfrak{P}}(\alpha) = \min_{a_i \neq 0} \{v_{\mathfrak{P}}(a_i\lambda^i)\} = \min_{a_i \neq 0} \{i + \Phi(M)v_{\mathfrak{P}}(a_i)\}.$$

En particular $v_{\mathfrak{P}}(a_i) \geq 0$ para toda $i = 0, 1, \dots, r$. Para cualquier $\sigma_A \in G_{P^n} = \text{Gal}(K(\Lambda_{P^n})/K)$, $\sigma_A(\lambda) = \lambda^A$, se tiene

$$\alpha_A := \sigma_A \alpha = a_0 + a_1\lambda^A + \dots + a_r(\lambda^A)^r$$

$A \bmod P^n \in (R_T/\langle P^n \rangle)^*$. Si $\{\bar{A}_1, \dots, \bar{A}_{\Phi(M)}\}$ es un conjunto de representantes de $(R_T/\langle P^n \rangle)^*$, poniendo $\alpha_i := \alpha^{A_i}$ y $\lambda_i = \lambda^{A_i}$ se obtiene

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{\Phi(M)} \end{pmatrix} = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^r \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_{r+1} & \lambda_{r+1}^2 & \cdots & \lambda_{r+1}^r \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_r \end{pmatrix}.$$

El determinante de la matriz $[\lambda_i^j]_{\substack{0 \leq j \leq r \\ 1 \leq i \leq r+1}}$ es un determinante de Vandermonde por lo que $\det [\lambda_i^j] = \prod_{1 \leq t \leq \ell \leq r+1} (\lambda_\ell - \lambda_t) := d$. Por tanto

$$a_i = \frac{\det \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{i-1} & \alpha_1 & \lambda_1^{i+1} & \cdots & \lambda_1^r \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_{r+1} & \cdots & \lambda_{r+1}^{i-1} & \alpha_1 & \lambda_{r+1}^{i+1} & \cdots & \lambda_{r+1}^r \end{bmatrix}}{\det \begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^r \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_{r+1} & \lambda_{r+1}^2 & \cdots & \lambda_{r+1}^r \end{bmatrix}} = \frac{b_i}{d}$$

con $b_i \in \mathcal{O}_M$. Por la demostración de la Proposición 9.2.23 $\lambda = \beta_A \lambda^A$ para $A \bmod P^n \in (R_T / \langle P^n \rangle)^*$ y $P = \beta_0 \lambda^{\Phi(P^n)}$, $\beta_n - \beta_0 \in \mathcal{O}_M$.

Entonces para cualquier divisor primo \mathfrak{q} en $K(\Lambda_M)$ que no divide ni a \mathfrak{p} ni a \mathfrak{p}_∞ , se tiene $v_{\mathfrak{p}}(\lambda) = v_{\mathfrak{p}}(\lambda^A) = 0$. Se sigue que el soporte del divisor de polos de a_i puede consistir solo de \mathfrak{p} y \mathfrak{p}_∞ . Sin embargo, puesto que $v_{\mathfrak{p}}(a_i) \geq 0$, se sigue que $a_i \in R_T$ y que $\mathcal{O}_M = R_T[\lambda]$. \square

El resultado general, se sigue de la Proposición 9.3.6 y del Teorema 3.2.29 (ver la demostración del Teorema 3.2.30).

Teorema 9.3.7. *Para cualquier $M \in R_T \setminus \{0\}$, si \mathcal{O}_M es la cerradura entera de R_T en $K(\Lambda_M)$ y λ es un generador de Λ_M , se tiene $\mathcal{O}_M = R_T[\lambda]$.* \square

También tenemos el resultado análogo a Corolario 5.1.3.

Definición 9.3.8. Sea $P \in R_T$ un polinomio mónico e irreducible y sea $A \in R_T$. Decimos que

$$\mu(A \bmod P) = M \in R_T$$

si M es mónico y de grado mínimo satisfaciendo $A^M \equiv 0 \bmod P$.

Observación 9.3.9. Sea $N \in R_T$ tal que $A^N \equiv 0 \bmod P$ y sea $N = QM + R$ con $Q, R \in R_T$ y $R = 0$ o $\text{gr } R < \text{gr } M$.

Entonces $A^N = (A^M)^Q + A^R$ por lo que $A^R \equiv 0 \bmod P$. Por tanto $R = 0$ y M divide a N . En particular el polinomio M dado en la Definición 9.3.8 es único.

Por otro, puesto que $R_T / \langle P \rangle$ es finito, el conjunto $\{A^M \bmod P \mid M \in R_T\}$ es también finito y por tanto existen dos elementos distintos $M_1, M_2 \in R_T$ tales que $A^{M_1} \equiv A^{M_2} \bmod P$. Por tanto $A^{M_1 - M_2} \equiv 0 \bmod P$ y $M_1 - M_2 \neq 0$.

Proposición 9.3.10. Sea $P \in R_T$ polinomio irreducible y $M \in R_T$ mónico no divisible por P . Si $A \in R_T$, entonces

$$P|\Psi_M(A) \iff \mu(A \bmod P) = M.$$

Demostración. Primero supongamos que $P|\Psi_M(A)$. Puesto que

$$u^M = \prod_{D|M} \Psi_D(u) \quad \text{se sigue que} \quad A^M = \prod_{D|M} \Psi_D(A) \equiv 0 \bmod P.$$

Sea $\mu(A \bmod P) = N$. Entonces $N|M$ y por tanto $A^N = \prod_{D|N} \Psi_D(A) \equiv 0 \bmod P$. Por lo tanto existe $D_0|N$ tal que $P|\Psi_{D_0}(A)$. Si $D_0 \neq M$, entonces

$$A^M = \Psi_M(A) \Psi_{D_0}(A) \prod_{\substack{D \neq D_0, M \\ D|M}} \Psi_D(A) \equiv 0 \bmod P^2.$$

En particular $u^M \bmod P$ tiene una raíz múltiple pero $(u^M)' = M \not\equiv 0 \bmod P$, es decir, $u^M \bmod P$ es separable. Esta contradicción prueba que $D_0 = M$ y $\mu(A \bmod P) = M$.

Recíprocamente, sea $\mu(A \bmod P) = M$. Entonces

$$A^M = \prod_{D|M} \Psi_D(A) \equiv 0 \bmod P.$$

Por tanto $P|\Psi_D(A)$ para algún $D|M$. Si $D \neq M$, $A^D = \prod_{D'|D} \Psi_{D'}(A) \equiv 0 \bmod P$ lo que contradice el hecho de que $\mu(A \bmod P) = M$. Por tanto $D = M$ y $P|\Psi_M(A)$. \square

Proposición 9.3.11. Sea $P \in R_T$ un polinomio irreducible y $M \in R_T$ un polinomio mónico tal que $P \nmid M$. Entonces P divide a $\Psi_M(A)$ para algún $A \in R_T$ si y solamente si $P \equiv 1 \bmod M$.

Demostración. Si $P|\Psi_M(A)$ para algún $A \in R_T$, entonces por la Proposición 9.3.10 se tiene que $\mu(A \bmod P) = M$. Ahora bien

$$u\Psi_P(u) = u^P = \sum_{i=0}^d \binom{P}{i} u^{q^i} \equiv u^{q^d} \bmod P$$

donde $d = \text{gr } P$, pues $\Psi_P(u) = \prod_{\text{mcd}(C,P)=1} (u - \lambda^C)$ y $\langle P \rangle = \langle \lambda \rangle^{\Phi(P)}$ (ver la

prueba de la Proposición 9.2.23). Por tanto $A^P \equiv A^{q^d} \bmod P$.

Ahora bien, $\Phi(P) = q^d - 1 = |(R_T/\langle P \rangle)^*|$ por lo que $P \nmid A$ entonces $A^{q^d-1} \equiv 1 \bmod P$ así que $A^{q^d} \equiv A \bmod P$. Si $P|A$, $A^{q^d} \equiv 0 \equiv A \bmod P$.

En cualquier caso tenemos $A^{q^d} \equiv A \bmod P$ y por tanto $A^P \equiv A \bmod P$, lo cual equivale a $A^P - A = A^{P-1} \equiv 0 \bmod P$. Puesto que $\mu(A \bmod P) = M$ se sigue que M divide a $P - 1$ lo cual implica que $P \equiv 1 \bmod M$.

Recíprocamente, supongamos ahora que $P \equiv 1 \pmod{M}$. Se tiene que $d = \text{gr}(P-1) = \text{gr } P$ y $u^{P-1} = \sum_{i=0}^d \binom{P-1}{i} u^{d-i}$. Por lo tanto $(u^{P-1})' \pmod{P} \equiv (P-1) \pmod{P} \equiv -1 \pmod{P} \not\equiv 0$ lo cual implica que el polinomio $u^{P-1} \pmod{P} \in (R_T/\langle P \rangle)[u]$ es separable.

Puesto que $\text{gr}_u u^{P-1} = q^d = |R_T/\langle P \rangle|$ y $A^{P-1} \equiv 0 \pmod{P}$ para todo $A \in R_T$, se sigue que

$$u^{P-1} \pmod{P} = \prod_{D|P-1} \Psi_D(u) \pmod{P} = \prod_{\substack{A \pmod{P} \\ A \in R_T}} (u - A) \pmod{P}.$$

Por lo tanto existe $A \in R_T$ tal que $\Psi_M(A) \equiv 0 \pmod{P}$. Se sigue que P divide a $\Psi_M(A)$ y que $\mu(A \pmod{P}) = M$. \square

Corolario 9.3.12 (Caso particular al Teorema de Dirichlet). *Sea $M \in R_T$ un polinomio mónico no constante. Entonces existen una infinidad de polinomios irreducibles $P \in R_T$ tales que $P \equiv 1 \pmod{M}$.*

Demostración. Sea $\{P_1, \dots, P_r\}$ un conjunto finito de cardinalidad $r \geq 0$ de polinomios irreducibles que satisfacen $P_i \equiv 1 \pmod{M}$. Sea $N := MP_1 \cdots P_r$ y sea $Q \in R_T$ arbitrario. Entonces $\Psi_M(NQ) \equiv \Psi_M(0) \pmod{N}$. Ahora bien, puesto que

$$\Psi_M(u) = \prod_{\substack{D|M \\ D \text{ mónico}}} (u^D)^{\mu(M/D)}, \quad \Psi_P(u) = \frac{u^P}{u}$$

(Proposición 9.2.21) y

$$\frac{u^M}{u} \Big|_{u=0} = \begin{bmatrix} M \\ 0 \end{bmatrix} = M,$$

entonces

$$\Psi_M(0) = \begin{cases} R & M = R^n \text{ para algún } R \text{ irreducible, } n \geq 1 \\ 1 & \text{en otro caso} \end{cases}.$$

Primero supongamos que M no es potencia de un polinomio irreducible, es decir, $\Psi_M(0) = 1$. Entonces $\Psi_M(NQ) \equiv 1 \pmod{N}$. Por lo tanto $\Psi_M(NQ) \equiv 1 \pmod{M}$ y $\Psi_M(NQ) \equiv 1 \pmod{P_i}$, $1 \leq i \leq r$. En particular, $P_i \nmid \Psi_M(NQ)$.

Sea P cualquier polinomio irreducible que divide a $\Psi_M(NQ)$. Entonces $P \equiv 1 \pmod{M}$ por la Proposición 9.3.11 y $P \neq P_i$.

Ahora si M es potencia de un irreducible, $M = R^n$, se tiene $P_i \neq R$, $1 \leq i \leq r$ y $\Psi_M(NQ) \equiv R \pmod{M}$; $\Psi_M(NQ) \equiv R \pmod{P_i}$. Si $P \mid \Psi_M(NQ)$ con P un polinomio irreducible, entonces si $P = P_i$ para algún i con $1 \leq i \leq r$.

De aquí se seguiría que $P_i | R$ lo cual implicaría que $P_i = R$ que es absurdo. Se sigue que $P \equiv 1 \pmod{M}$ y $P \neq P_i$ para todo i , $1 \leq i \leq r$ (si $r = 0$ la condición es vacía). \square

Observación 9.3.13. El Corolario 9.3.12 es un caso particular del Teorema de Dirichlet sobre la infinitud de polinomios irreducibles en progresiones geométricas (ver Teorema 9.3.14) y el cual es consecuencia del Teorema de Densidad de Cebotarev el cual no probaremos aquí.

Teorema 9.3.14 (Dirichlet). Sean $M, N \in R_T$ cualesquiera dos polinomios mónicos no constantes primos relativos. Entonces existe un infinitud de polinomios irreducibles $P \in R_T$ tales que $P \equiv N \pmod{M}$. \square

9.4. Caracteres de Dirichlet

Definición 9.4.1. Sea $M \in R_T \setminus \{0\}$ un polinomio mónico. Un *caracter de Dirichlet módulo M* es un homomorfismo

$$\chi: (R_T/\langle M \rangle)^* \longrightarrow \mathbb{C}^*.$$

Observación 9.4.2. Si M divide a N en R_T , tenemos el epimorfismo canónico

$$\begin{aligned} \varphi_{N,M}: (R_T/\langle N \rangle)^* &\twoheadrightarrow (R_T/\langle M \rangle)^* \\ A \pmod{N} &\mapsto A \pmod{M}. \end{aligned}$$

Entonces para todo caracter de Dirichlet módulo M , $\chi: (R_T/\langle M \rangle)^* \rightarrow \mathbb{C}^*$, $\varphi_{N,M}$ induce un caracter de Dirichlet módulo N : $\chi \circ \varphi_{N,M}: (R_T/\langle N \rangle)^* \rightarrow \mathbb{C}^*$,

$$\begin{array}{ccc} (R_T/\langle N \rangle)^* & \xrightarrow{\chi \circ \varphi_{N,M}} & \mathbb{C}^* \\ & \searrow \varphi_{N,M} \quad \nearrow \chi & \\ & (R_T/\langle M \rangle)^* & \end{array}$$

Recíprocamente, si χ es un caracter de Dirichlet módulo M , decimos que podemos definir χ módulo F para $F|M$ si existe $\xi: (R_T/\langle F \rangle)^* \rightarrow \mathbb{C}^*$ tal que $\xi \circ \varphi_{M,F} = \chi$.

$$\begin{array}{ccc} (R_T/\langle M \rangle)^* & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{M,F} \quad \nearrow \xi & \\ & (R_T/\langle F \rangle)^* & \end{array}$$

(Señalando la relación $\xi \circ \varphi_{M,F} = \chi$ con una flecha circular)

Observación 9.4.3. Si χ es un caracter de Dirichlet definido módulo $M \in R_T$, entonces si $F|M$, $F \in R_T$, se tiene que χ se puede definir módulo F si y solamente si $\chi(A \bmod M) = \chi(B \bmod M)$ para cualesquiera $A, B \in R_T$ primos relativos a M y tales que $A \equiv B \bmod F$.

Teorema 9.4.4 (Existencia del conductor). Sea χ un caracter de Dirichlet definido módulo M . Entonces existe un polinomio mónico único F en R_T de grado mínimo que divide a M tal que χ puede ser definido módulo F .

Demostración. Sea $\chi: (R_T/\langle M \rangle)^* \rightarrow \mathbb{C}^*$. Sean $A, B \in R_T$ mónicos que dividen a M y tales que χ puede ser definido módulo A y también módulo B , es decir, existen $\chi_A: (R_T/\langle A \rangle)^* \rightarrow \mathbb{C}^*$ y $\chi_B: (R_T/\langle B \rangle)^* \rightarrow \mathbb{C}^*$ tales que $\chi = \chi_A \circ \varphi_{M,A}$, $\chi = \chi_B \circ \varphi_{M,B}$. Consideremos $C := \text{mcd}(A, B)$ el máximo común divisor de A y B . Sea D el producto de todos los polinomios mónicos irreducibles que dividen a M pero que no dividen a B . Entonces $C = \text{mcd}(DA, B)$. Para ver que podemos definir χ módulo C , consideremos $U, V \in R_T$ primos relativos a M tales que $U \equiv V \bmod C$. Por el Teorema Chino del Residuo, existe $S \in R_T$ tal que $S \equiv U \bmod DA$ y $S \equiv V \bmod B$.

Veamos que S y M son primos relativos. En caso contrario existiría $P \in R_T$ irreducible que divide a S y a M . Sea $S = V + QB$, entonces si $P|B$, entonces $P|V$ pero en este caso se seguiría que $P|\text{mcd}(V, M) = 1$ lo cual es absurdo, esto es, $P \nmid B$. Ahora bien, puesto que $P|M$ y $P \nmid B$ entonces P es un factor de D y por lo tanto $P|DA$. Pero $P|S$ por lo cual $P|U$ y por lo tanto $P|\text{mcd}(U, M) = 1$ lo cual es absurdo. En resumen, $\text{mcd}(S, M) = 1$. Entonces

$$\chi(S) = \chi_A \circ \varphi_{M,A}(S) = \chi_A \circ \varphi_{M,A}(U) = \chi(U)$$

y

$$\chi(S) = \chi_B \circ \varphi_{M,B}(S) = \chi_B \circ \varphi_{M,B}(V) = \chi(V).$$

Por lo tanto $\chi(S) = \chi(U) = \chi(V)$ de donde χ puede ser definido módulo C :

$$\begin{array}{ccc} (R_T/\langle M \rangle)^* & \xrightarrow{\chi} & \mathbb{C}^* \\ & \searrow \varphi_{M,C} & \nearrow \chi_C \\ & (R_T/\langle C \rangle)^* & \end{array}$$

Finalmente si χ puede ser definido módulo F_1 y módulo F_2 con F_1 y F_2 de grado mínimo y F_1, F_2 mónicos, entonces χ puede ser definido módulo $C = \text{mcd}(F_1, F_2)$. Puesto que $C|F_1$ y $C|F_2$ se sigue que $C = F_1$ y $C = F_2$, es decir, $F_1 = F_2$. \square

Definición 9.4.5. El polinomio dado en el Teorema 9.4.4 se llama *conductor* de χ y se denota por F_χ . En otras palabras, si χ es un caracter de Dirichlet definido módulo M , entonces F_χ es el único polinomio de grado mínimo que divide a M y tal que χ puede definirse módulo F_χ .

Observación 9.4.6. Sean $q = 2$ y $M \in R_T \setminus \{0\}$ mónico tal que $\text{mcd}(M, T) = \text{mcd}(M, T+1) = 1$. Entonces no existe ningún caracter de Dirichlet θ tal que $F_\theta = TM$ ni $F_\theta = (T+1)M$.

En efecto notemos que $\Phi(MT) = \Phi(M)\Phi(T) = \Phi(M)$ y $\Phi(M(T+1)) = \Phi(M)\Phi(T+1) = \Phi(M)$ ya que $\Phi(T) = \Phi(T+1) = 1$ pues estamos en el caso $q = 2$. Entonces

$$(R_T/\langle TM \rangle)^* \cong (R_T/\langle (T+1)M \rangle)^* \cong (R_T/\langle M \rangle)^*.$$

En particular, con $M = 1$, vemos que para $q = 2$ no hay caracter de conductor T , $T+1$ o $T(T+1)$.

Ejemplo 9.4.7. Sea $q = 2$ y sea $\chi: (R_T/\langle T^3 \rangle)^* \rightarrow \mathbb{C}^*$ dado por

$$\begin{aligned} 1 &\mapsto 1, \\ T+1 &\mapsto -1, \\ T^2+1 &\mapsto 1, \\ T^2+T+1 &\mapsto -1. \end{aligned}$$

Puesto que $\chi(T^2+A) = \chi(A)$ para toda $A \in (R_T/\langle T^3 \rangle)^*$ entonces χ se puede definir módulo T^2 pues si $\xi: (R_T/\langle T^2 \rangle)^* \rightarrow \mathbb{C}^*$, $\xi(1) = 1$, $\xi(1+T) = -1$ y $\varphi_{T^3, T^2}: (R_T/\langle T^3 \rangle)^* \rightarrow (R_T/\langle T^2 \rangle)^*$, entonces

$$\begin{aligned} \varphi_{T^3, T^2}(1) &= \varphi_{T^3, T^2}(T^2+1) = 1 \quad \text{y} \\ \varphi_{T^3, T^2}(T+1) &= \varphi_{T^3, T^2}(T^2+T+1) = T+1 \end{aligned}$$

se sigue que $\xi \circ \varphi_{T^3, T^2} = \chi$. Por la Observación 9.4.6, se tiene que $F_\chi = T^2$.

Ejemplo 9.4.8. Sea $q = 2$ y sea $\chi: (R_T/\langle T^2(T+1) \rangle)^* \rightarrow \mathbb{C}^*$ dado por $\chi(1) = 1$ y $\chi(T^2+T+1) = -1$. Entonces si $\xi: (R_T/\langle T^2 \rangle)^* \rightarrow \mathbb{C}^*$, $\xi(1) = 1$, $\xi(1+T) = -1$ satisface $\xi \circ \varphi_{T^2(T+1), T^2} = \chi$. Por lo tanto $F_\chi = T^2$.

La misma conclusión puede obtenerse usando dos veces la Observación 9.4.6: $(R_T/\langle T^2(T+1) \rangle)^* \cong (R_T/\langle T^2 \rangle)^*$.

Ejemplo 9.4.9. Sea $q = 2$, $N = T^2 + T + 1$, $M = NT$, $\omega = e^{2\pi i/3}$ y $\theta: (R_T/\langle M \rangle)^* \rightarrow \mathbb{C}^*$ dado por

$$\begin{aligned} 1 &\mapsto 1, \\ T^2+1 &\mapsto \omega, \\ T+1 &\mapsto \omega^2. \end{aligned}$$

Puesto que $(R_T/\langle NT \rangle)^* \cong (R_T/\langle N \rangle)^*$, se pueden definir $\tilde{\theta}: (R_T/\langle N \rangle)^* \rightarrow \mathbb{C}^*$, $\tilde{\theta}(1) = 1$, $\tilde{\theta}(T) = \theta(T^2+1) = \omega$ y $\tilde{\theta}(T+1) = \omega^2$. Por lo tanto $F_\theta = T^2+T+1$.

Observación 9.4.10. Dado un caracter de Dirichlet podemos considerar χ como un mapeo $\chi: R_T \rightarrow \mathbb{C}$ definiendo $\chi(Q) = 0$ si $\text{mcd}(Q, F_\chi) \neq 1$. En caso de no especificarse, siempre consideraremos a un caracter χ definido módulo su conductor F_χ .

Definición 9.4.11. Un caracter de Dirichlet χ definido módulo su conductor se llama *primitivo*. En este caso se hace $\chi(Q) = 0$ tan poco como sea posible.

También notemos que cuando χ está definido módulo su conductor, tenemos que $\chi(A + F_\chi) = \chi(A)$, esto es, χ es periódico de período F_χ .

Notación 9.4.12. Siempre que mencionemos los caracteres de $(R_T/\langle M \rangle)^*$, $M \in R_T$ o *caracteres módulo M* incluiremos todos los caracteres cuyos conductores dividan a M . El *caracter trivial* ε satisface $\varepsilon(Q) = 1$ para todo $Q \in R_T$. Si G es cualquier grupo, \hat{G} denota al conjunto de sus caracteres: $\hat{G} := \text{Hom}(G, \mathbb{C}^*) = \{\chi: G \rightarrow \mathbb{C}^* \mid \chi \text{ es homomorfismo de grupos}\}$.

Definición 9.4.13. Diremos que un caracter es *par* si $\theta(a) = 1$ para todo $a \in \mathbb{F}_q^*$.

Proposición 9.4.14. Sea $X := \{\theta \in (\widehat{R_T/\langle N \rangle})^* \mid \theta \text{ es par}\}$. Entonces X es subgrupo de $(\widehat{R_T/\langle N \rangle})^*$ de orden $\frac{\Phi(N)}{q-1}$.

Demostración. Se tiene la sucesión exacta

$$0 \longrightarrow \mathbb{F}_q^* \longrightarrow (\widehat{R_T/\langle N \rangle})^*.$$

Tomando duales, se obtiene la sucesión exacta

$$\begin{aligned} (\widehat{R_T/\langle N \rangle})^* &\xrightarrow{\mathfrak{X}} \mathbb{F}_q^* \longrightarrow 0 \\ \theta &\longmapsto \theta|_{\mathbb{F}_q^*} \end{aligned}$$

Se tiene que $X = \text{nuc } \mathfrak{X}$ y por tanto $(\widehat{R_T/\langle N \rangle})^*/X \cong \mathbb{F}_q^*$ de donde se sigue que

$$|X| = \frac{|(\widehat{R_T/\langle N \rangle})^*|}{|\mathbb{F}_q^*|} = \frac{|(R_T/\langle N \rangle)^*|}{|\mathbb{F}_q^*|} = \frac{\Phi(N)}{q-1}. \quad \square$$

Definición 9.4.15. Sean χ, ϕ dos caracteres de Dirichlet de conductores F_χ y F_ϕ respectivamente. Se define el producto de χ y ϕ como sigue. Sea $Q := [F_\chi, F_\phi]$ y se define $\gamma: (\widehat{R_T/\langle Q \rangle})^* \rightarrow \mathbb{C}^*$ por $\gamma(A \bmod Q) = \chi(A \bmod Q)\phi(A \bmod Q)$. Entonces el *producto* $\chi\phi$ se define como el caracter primitivo asociado a γ . En particular $F_{\chi\phi} | [F_\chi, F_\phi]$.

Teorema 9.4.16. Si $\text{mcd}(F_\chi, F_\phi) = 1$ entonces $F_{\chi\phi} = F_\chi F_\phi$.

Demostración. Sean $N = F_\chi$, $M = F_\phi$, $S := [N, M] = NM$. Definimos $\gamma: (R_T/\langle S \rangle)^* \rightarrow \mathbb{C}^*$ dada por $\gamma(A \bmod S) = \gamma(A \bmod S)\phi(A \bmod S)$.

Ahora bien, puesto que $[S, N] = S$ se puede definir $\theta: (R_T/\langle S \rangle)^* \rightarrow \mathbb{C}^*$ por $\theta(A \bmod S) = \gamma(A \bmod S)\chi^{-1}(A \bmod S)$. Se obtiene $\theta = \phi \bmod S$ lo que implica que $F_\theta = F_\phi = M$. Por lo tanto $M = F_\theta = F_{\gamma\chi^{-1}}|[F_\gamma, F_{\chi^{-1}}]$.

Es decir, $M|[F_\gamma, F_{\chi^{-1}}] = [F_\gamma, F_\theta] = \frac{F_\gamma N}{\text{mcd}(F_\gamma, N)} = F_\gamma N_1$ donde $N_1 = \frac{N}{\text{mcd}(F_\gamma, N)}$. Puesto que $\text{mcd}(N, M) = 1$ se sigue que $\text{mcd}(N_1, M) = 1$ y $M|F_\gamma$. Análogamente $N|F_\gamma$ y puesto que $\text{mcd}(N, M) = 1$, se tiene que $NM|F_\gamma$. Por otro lado $F_\gamma = F_{\chi\phi}[F_\chi, F_\phi] = [N, M] = NM$. Se sigue que $F_\gamma = NM = F_\chi F_\phi$. \square

Proposición 9.4.17. Sean χ, σ dos caracteres de Dirichlet de conductores F_χ y F_σ respectivamente. Supongamos que existe N tal que $F_\chi|N$, $F_\sigma|N$ y $\chi, \sigma: (R_T/\langle N \rangle)^* \rightarrow \mathbb{C}^*$ son iguales módulo N , es decir, $\chi(A \bmod N) = \sigma(A \bmod N)$ para todo A primo relativo a N . Entonces $F_\chi = F_\sigma$ y $\chi = \sigma \bmod F_\chi$, esto es, $\chi = \sigma$.

Demostración. Consideremos

$$\begin{array}{ccc} (R_T/\langle N \rangle)^* & \xrightarrow{\chi} & \mathbb{C}^* \\ \varphi_{N, F_\chi} \downarrow & \nearrow \tilde{\chi} & \\ (R_T/\langle F_\chi \rangle)^* & & \end{array}$$

Tenemos $\tilde{\chi} \circ \varphi_{N, F_\chi} = \chi = \sigma$, es decir, σ se puede definir módulo F_χ lo cual implica que $F_\sigma|F_\chi$. Por simetría, se tiene que $F_\chi|F_\sigma$ y por tanto $F_\chi = F_\sigma$. Sean $\chi' \equiv \chi \bmod F_\chi$, $\sigma' \equiv \sigma \bmod F_\sigma$. Sea $A \in R_T \setminus \{0\}$ tal que $\text{mcd}(A, F_\chi) = 1$. Existe $A' \in R_T$ tal que $\text{mcd}(A, N) = 1$ y $A \bmod F_\chi = A' \bmod F_\chi$. Luego $\chi'(A \bmod F_\chi) = \chi'(A' \bmod F_\chi) = \chi(A' \bmod N) = \sigma(A' \bmod N) = \sigma(A' \bmod F_\chi) = \sigma'(A \bmod F_\chi)$. \square

Observación 9.4.18. En general no se tiene que $(\chi\phi)(\overline{A}) = \chi(\overline{A})\phi(\overline{A})$.

Ejemplo 9.4.19. Sea $q = 2$ y sea χ módulo $T^2(T^2 + 1)$ dado por

$$\chi(1) = 1, \quad \chi(T^2 + T + 1) = 1, \quad \chi(T^3 + T^2 + 1) = -1, \quad \chi(T^3 + T + 1) = -1.$$

Por la Observación 9.4.6 se tiene que el conductor de χ , $F_\chi \in \{1, T^2, T^2 + 1, T^2(T^2 + 1)\}$. Como $\chi(T^3 + T^2 + 1) = -1$, $F_\chi \neq 1$.

Ahora $T^3 + T^2 + 1 \bmod T^2 = 1$ pero $\chi(T^3 + T^2 + 1) = -1 \neq 1$ y $T^3 + T + 1 \bmod (T^2 + 1) = 1$ pero $\chi(T^3 + T + 1) = -1 \neq 1$, por lo que $F_\chi \neq T^2, T^2 + 1$. Se sigue que $F_\chi = T^2(T^2 + 1)$.

Ahora sea $\varphi \bmod T^2$ dada por $\varphi(1) = 1$, $\varphi(1 + T) = -1$. Por tanto $F_\varphi = T^2$.

Consideremos el producto $\chi\varphi$. Se tiene que $[F_\chi, F_\varphi] = [T^2(T^2+1), T^2] = T^2(T^2+1)$ y definimos $\gamma: (R_T/T^2(T^2+1))^* \rightarrow \mathbb{C}^*$ por $\gamma(A) = \chi(A)\varphi(A)$. Entonces

$$\begin{aligned}\gamma(1) &= \chi(1)\varphi(1) = 1 \cdot 1 = 1, \\ \gamma(T^2 + T + 1) &= \chi(T^2 + T + 1)\varphi(T^2 + T + 1) = (1)(-1) = -1, \\ \gamma(T^3 + T^2 + 1) &= \chi(T^3 + T^2 + 1)\varphi(T^3 + T^2 + 1) = (-1)(1) = -1, \\ \gamma(T^3 + T + 1) &= \chi(T^3 + T + 1)\varphi(T^3 + T + 1) = (-1)(-1) = 1.\end{aligned}$$

Sea $\xi: (R_T/\langle T^2 + 1 \rangle)^* \rightarrow \mathbb{C}^*$ dado por $\xi(1) = 1$ y $\xi(T) = 1$. Entonces $\xi \circ \varphi_{T^2(T^2+1), T^2+1} = \gamma$. Por tanto $F_\gamma = T^2 + 1$ y $\xi = \chi\phi$. Notemos que $\xi(T) = -1 \neq 0 = \varphi(T) = \chi(T)\varphi(T)$.

Ejemplo 9.4.20. Sean $q = 2$, $\zeta = \zeta_6 = e^{2\pi i/6}$, $\omega = \zeta_3 = e^{2\pi i/3}$, $M = T^2N$ con $N = T^2 + T + 1$. Definimos

$$\begin{array}{ll}\chi: (R_T/\langle M \rangle)^* \longrightarrow \mathbb{C}^* & \\ 1 \longmapsto 1 & \\ T + 1 \longmapsto \zeta & \\ T^2 + 1 \longmapsto \zeta^2 & \\ T^3 + T^2 + T + 1 \longmapsto -1 & \\ T^3 + T^2 + 1 \longmapsto -\zeta & \\ T^3 + T + 1 \longmapsto -\zeta^2 & \end{array} \quad \begin{array}{ll}\sigma: (R_T/\langle T^2 \rangle)^* \longrightarrow \mathbb{C}^* & \\ 1 \longmapsto 1 & \\ T + 1 \longmapsto -1 & \end{array}$$

Se tiene $F_\chi = M$, $F_\sigma = T^2$ y por tanto $[F_\chi, F_\sigma] = M$. Obtenemos ψ mód M :

$$\begin{array}{lll}(R_T/\langle M \rangle)^* \longrightarrow (R_T/\langle T^2 \rangle)^* \longrightarrow \mathbb{C}^* & & \\ 1 \longmapsto 1 & 1 \longmapsto 1 & \\ T + 1 \longmapsto T + 1 & \longmapsto -1 & \\ T^2 + 1 \longmapsto 1 & \longmapsto 1 & \\ T^3 + T^2 + T + 1 \longmapsto T + 1 & \longmapsto -1 & \\ T^3 + T^2 + 1 \longmapsto 1 & \longmapsto 1 & \\ T^3 + T + 1 \longmapsto T + 1 & \longmapsto -1. & \end{array}$$

Ahora sea $\gamma: (R_T/\langle M \rangle)^* \rightarrow \mathbb{C}^*$ dada por

$$\gamma(A) = \chi(A)\sigma(A) = \begin{cases} 1 & \text{si } A = 1 \\ \omega^2 & \text{si } A = T + 1 \\ \omega & \text{si } A = T^2 + 1 \\ 1 & \text{si } A = T^3 + T^2 + T + 1 \\ \omega^2 & \text{si } A = T^3 + T^2 + 1 \\ \omega & \text{si } A = T^3 + T + 1 \end{cases}$$

Podemos definir γ módulo N :

$$\begin{array}{lll}
(R_T/\langle M \rangle)^* & \longrightarrow & (R_T/\langle N \rangle)^* \longrightarrow \mathbb{C}^* \\
1 & \longmapsto & 1 \longmapsto 1 \\
T+1 & \longmapsto & T+1 \longmapsto \omega^2 \\
T^2+1 & \longmapsto & T \longmapsto \omega \\
T^3+T^2+T+1 & \longmapsto & 1 \longmapsto 1 \\
T^3+T^2+1 & \longmapsto & T+1 \longmapsto \omega^2 \\
T^3+T+1 & \longmapsto & T \longmapsto \omega.
\end{array}$$

El producto de caracteres χ y σ es:

$$\begin{array}{ll}
\chi\sigma: (R_T/\langle N \rangle)^* & \longrightarrow \mathbb{C}^* \\
1 & \longmapsto 1 \\
T & \longmapsto \omega \\
T+1 & \longmapsto \omega^2
\end{array}$$

y $F_{\chi\sigma} = N$. Notemos que $(\chi\sigma)(T) = \omega \neq 0 = \chi(T)\sigma(T)$.

Definición 9.4.21. Si χ es un caracter de Dirichlet, definimos el *conjugado* $\bar{\chi}$ de χ por $\bar{\chi}(A) = \overline{\chi(A)}$. Notemos que $\bar{\chi}(A) = \chi(A)^{-1}$ para toda $\text{mcd}(A, F_\chi) = 1$. Por tanto $\chi\bar{\chi}$ es el caracter trivial y $F_{\bar{\chi}} = F_\chi$.

Observación 9.4.22. Tenemos $G_M = \text{Gal}(K(\Lambda_M)/K) \cong (R_T/\langle M \rangle)^*$. Entonces un caracter de Dirichlet módulo M es un caracter de G_M , por lo que el caracter de Dirichlet puede ser considerado un *caracter de Galois*.

Definición 9.4.23. Sea χ un caracter de Dirichlet módulo M , esto es, $\chi \in \widehat{G_M} \cong (R_T/\langle M \rangle)^*$. Entonces $\text{nuc } \chi \subseteq G_M$. Sea $K_\chi := K(\Lambda_M)^{\text{nuc } \chi}$. El campo K_χ se llama el *campo perteneciente a χ* o que K_χ *está asociado a χ* .

Ejemplo 9.4.24. Sea χ el caracter del Ejemplo 9.4.7. Entonces

$$\begin{array}{l}
\chi: (R_T/\langle T^3 \rangle)^* \cong G_{T^3} = \text{Gal}(K(\Lambda_{T^3})/K) \rightarrow \mathbb{C}^* \quad \text{y} \\
\text{nuc } \chi = \{1 \text{ mód } T^3, (T^2+1) \text{ mód } T^3\}.
\end{array}$$

Por lo tanto χ es un caracter de $(R_T/\langle T^3 \rangle)^*/\text{nuc } \chi \cong (R_T/\langle T^2 \rangle)^* \cong \text{Gal}(K(\Lambda_{T^2})/K)$ y puede ser considerado un caracter de $\text{Gal}(K(\Lambda_{T^2})/K)$.

Ejemplo 9.4.25. Sea χ el caracter del Ejemplo 9.4.8. Entonces $(R_T/\langle T^2(T+1) \rangle)^* \cong (R_T/\langle T^2 \rangle)^*$ y puesto que cualquier caracter módulo $T^2(T+1)$ o módulo T^2 es el mismo caracter, se sigue que $K(\Lambda_{T^2(T+1)}) = K(\Lambda_{T^2})$.

Observación 9.4.26. Se puede probar que el grupo de inercia del primo infinito es $\mathbb{F}_q^* \subseteq G_M \cong (R_T/\langle M \rangle)^*$. Por lo tanto χ es par si y solamente si \mathfrak{p}_∞ se descompone totalmente en K_χ/K .

Definición 9.4.27. Al campo $K(\Lambda_M)^+ := K(\Lambda_M)^{\mathbb{F}_q^*}$ se le llama *el máximo subcampo real de $K(\Lambda_M)$* .

Se tiene $[K(\Lambda_M) : K(\Lambda_M)^+] = |\mathbb{F}_q^*| = q - 1$ y \mathfrak{p}_∞ se descompone totalmente en $\Phi(M)/(q - 1)$ divisores en $K(\Lambda_M)^+/K$.

Como en el caso numérico (ver Teorema 5.3.2), el comportamiento de la extensión $K(\Lambda_M)/K(\Lambda_M)^+$ es diferente cuando M es potencia de un polinomio irreducible que cuando hay al menos dos primos distintos dividiendo a M como veremos a continuación.

Sea $M = \prod_{i=1}^r P_i^{\alpha_i}$ como producto de polinomios irreducibles. Sean \mathfrak{p}_∞ el primo infinito en K y \mathfrak{P}_∞ un primo en $K(\Lambda_M)$ dividiendo a \mathfrak{p}_∞ . Se tiene $e(\mathfrak{P}_\infty|\mathfrak{p}_\infty) = q - 1$ y $I(\mathfrak{P}_\infty|\mathfrak{p}_\infty) = \mathbb{F}_q^*$. Por lo tanto \mathfrak{p}_∞ es no ramificado en $K(\Lambda_M)^+/K$ y \mathfrak{P}_∞ es totalmente ramificado en $K(\Lambda_M)/K(\Lambda_M)^+$. Por otro lado, si $\mathfrak{Q}_\infty^{(i)}$ denota un primo en $K(\Lambda_{P_i^{\alpha_i}})$ dividiendo a \mathfrak{p}_∞ , se tiene $e(\mathfrak{Q}_\infty^{(i)}|\mathfrak{p}_\infty) = q - 1$.

Lema 9.4.28. *Se tiene $K(\Lambda_M) = K(\Lambda_M)^+(\Lambda_{P_i})$.*

Demostración. Sea $F := K(\Lambda_M)^+(\Lambda_{P_i})$, $F \subseteq K(\Lambda_M)$. Se tiene $[K(\Lambda_M) : K(\Lambda_M)^+] = q - 1 = |\mathbb{F}_q^*|$. Con las notaciones naturales, tenemos:

$$e_{F/K}(\mathfrak{p}_\infty) = e_{F/K(\Lambda_M)^+}(\mathfrak{p}_\infty)e_{K(\Lambda_M)^+/K}(\mathfrak{p}_\infty) = e_{F/K(\Lambda_M)^+}(\mathfrak{p}_\infty).$$

Por otro lado, puesto que $K \subseteq K(\Lambda_{P_i}) \subseteq F$, se tiene $e_{F/K}(\mathfrak{p}_\infty) \geq e_{K(\Lambda_{P_i})/K}(\mathfrak{p}_\infty) = q - 1$. Por lo tanto

$$\begin{aligned} e_{F/K(\Lambda_M)^+}(\mathfrak{p}_\infty) &\geq q - 1 = [K(\Lambda_M) : K(\Lambda_M)^+] \\ &\geq [F : K(\Lambda_M)^+] \geq e_{F/K(\Lambda_M)^+}(\mathfrak{p}_\infty), \end{aligned}$$

de donde se sigue que

$$e_{F/K(\Lambda_M)^+}(\mathfrak{p}_\infty) = [F : K(\Lambda_M)^+] = q - 1 = [K(\Lambda_M) : K(\Lambda_M)^+].$$

Por lo tanto $F = K(\Lambda_M)$. □

Corolario 9.4.29. *En $K(\Lambda_M) = K(\Lambda_M)^*(\Lambda_{P_i})$, el único posible primo finito ramificado es P_i .* □

Corolario 9.4.30. *Si $r \geq 2$, no hay ningún primo finito ramificado.* □

Observación 9.4.31. Si $r = 1$, $M = P_1^{\alpha_1}$, P_1 es ramificado en la extensión $K(\Lambda_M)/K(\Lambda_M)^+$, excepto en el caso $q = 2$, $\alpha_1 = 1$ y $P_1 = T$ o $P_1 = T + 1$.

Observación 9.4.32. En cualquier caso, excepto $q = 2$, \mathfrak{p}_∞ es ramificado en $K(\Lambda_M)/K(\Lambda_M)^+$.

Ejemplo 9.4.33. Sean $q = 3$, $M = T^2 + 1$, $\zeta = \zeta_8 = e^{2\pi i/8}$. Se tiene que $\Phi(M) = 8$, $(R_T/\langle M \rangle)^* = \{1, T+1, -T, -T+1, -1, -T-1, T, T-1\}$ y $\Lambda_M = \{u \in \overline{K} \mid u^M = 0\} = \{u \in \overline{K} \mid ((\varphi + \mu_T)^2 + \text{Id})(u) = 0\} = \{u \in \overline{K} \mid u^9 + (Tu)^3 + Tu^3 + T^2u + u = 0\}$. Entonces $u(u^8 + T^3u^2 + Tu^2 + 1) = 0$. Por lo tanto

$$\Psi_M(u) = u^8 + T^3u^2 + Tu^2 + T^2 + 1 = u^8 + (T^3 + T)u^2 + (T^2 + 1).$$

Sea λ una raíz de $\Psi_M(u)$ y sean $\sigma_1 = \text{Id}$, $\sigma_{-1}: \lambda \mapsto -\lambda$, $K(\Lambda_M)^+ = \{u \in K(\Lambda_M) \mid \sigma_{-1}(u) = u\}$ Puesto que

$$K(\Lambda_M) = \{A_0 + A_1\lambda + \cdots + A_7\lambda^7 \mid A_i \in K\}$$

tenemos

$$K(\Lambda_M)^+ = \{A_0 + A_2\lambda^2 + A_4\lambda^4 + A_6\lambda^6 \mid A_i \in K\}.$$

Sea

$$\begin{array}{ccc} \theta: (R_T/\langle M \rangle)^* \longrightarrow \mathbb{C}^* & & \theta^2: (R_T/\langle M \rangle)^* \longrightarrow \mathbb{C}^* \\ 1 \mapsto 1 & & 1 \mapsto 1 \\ T+1 \mapsto \zeta & & T+1 \mapsto i \\ -T \mapsto \zeta^2 = i & & -T \mapsto -1 \\ -T+1 \mapsto \zeta^3 & \text{luego} & -T+1 \mapsto -i \\ -1 \mapsto \zeta^4 = -1 & & -1 \mapsto 1 \\ -T-1 \mapsto \zeta^5 & & -T-1 \mapsto i \\ T \mapsto \zeta^6 & & T \mapsto -1 \\ T-1 \mapsto \zeta^7 & & T-1 \mapsto -i. \end{array}$$

Por lo tanto $\text{nuc } \theta^2 = \{1, -1\} \cong \{\sigma_1, \sigma_{-1}\} = J < G = G_M = \text{Gal}(K(\Lambda_M)/K)$ luego $K(\Lambda_M)^+ = K(\Lambda_M)^{\text{nuc } \theta^2}$. Entonces $K(\Lambda_M)^+$ es el campo perteneciente a θ^2 .

Observación 9.4.34. Sea χ un caracter de Dirichlet definido módulo M y sea $N \in R_T \setminus \{0\}$ un múltiplo de M . Sea $\tilde{\chi}$ el caracter χ definido módulo N , es decir,

$$\begin{array}{ccc} (R_T/\langle N \rangle)^* & \xrightarrow{\tilde{\chi}} & \mathbb{C}^* \\ & \searrow \varphi_{N,M} & \nearrow \chi \\ & (R_T/\langle M \rangle)^* & \end{array} \quad \tilde{\chi} = \chi \circ \varphi_{N,M}.$$

Sean $K_1 = K(\Lambda_M)^{\text{nuc } \chi}$ y $K_2 = K(\Lambda_M)^{\text{nuc } \tilde{\chi}}$. Entonces

$$\text{nuc } \varphi_{N,M} = D_{N,M} = \{A \text{ mód } N \mid A \equiv 1 \text{ mód } M\},$$

$(R_T/\langle N \rangle)^* / \text{núc } \varphi_{N,M} \cong (R_T/\langle M \rangle)^*$. Puesto que $G_N \cong (R_T/\langle N \rangle)^*$ y $G_M \cong (R_T/\langle M \rangle)^*$, $H = \text{Gal}(K(\Lambda_N), K(\Lambda_M))$

$$\left. \begin{array}{c} K(\Lambda_N) \\ \downarrow \\ K(\Lambda_M) \\ \downarrow G_M \\ K \end{array} \right\}^H \quad G_N \quad \begin{array}{l} \text{Entonces } K(\Lambda_M) = K(\Lambda_N)^H \text{ y} \\ \text{núc } \varphi_{N,M} \cong \text{Gal}(K(\Lambda_N)/K(\Lambda_M)) \cong H. \end{array}$$

Ahora bien, $\text{núc } \tilde{\chi} = \varphi_{N,M}^{-1}(\text{núc } \chi)$ y ya que $\varphi_{N,M}^{-1}(\text{núc } \chi) \supseteq \varphi_{N,M}^{-1}(\{1\}) = \text{núc } \varphi_{N,M}$ se sigue que

$$K_2 = K(\Lambda_N)^{\text{núc } \tilde{\chi}} \subseteq K(\Lambda_N)^{\text{núc } \varphi_{N,M}} = K(\Lambda_M).$$

Por tanto $K_2 \subseteq K(\Lambda_M)^{\text{núc } \chi} = K_1$. Por otro lado

$$\begin{aligned} |\text{núc } \tilde{\chi}| &= |\varphi_{N,M}^{-1}(\text{núc } \chi)| = |\text{núc } \varphi_{N,M}| |\text{núc } \chi| \\ &= [K(\Lambda_N) : K(\Lambda_M)] [K(\Lambda_M) : K_1] = [K(\Lambda_N) : K_1] \end{aligned}$$

y $|\text{núc } \tilde{\chi}| = [K(\Lambda_N) : K_2]$. Se sigue que $K_1 = K_2$.

Lo anterior implica que, dado cualquier caracter de Dirichlet χ definido módulo M , sin importar su conductor, el campo $K_{\chi,M} = K(\Lambda_M)^{\text{núc } \chi}$ depende únicamente de χ y no de M .

Definición 9.4.35. Sea X cualquier grupo finito de caracteres de Dirichlet. Sea M el mínimo común múltiplo de $\{F_\chi \mid \chi \in X\}$. Entonces X es un subgrupo de $\widehat{G_M}$. Sean $H := \bigcap_{\chi \in X} \text{núc } \chi$ y $K_X := K(\Lambda_M)^H$. Entonces K_X se llama *el campo que pertenece a X* o *el campo asociado a X* .

Se tiene que si X es cíclico, $X = \langle \chi \rangle$, entonces $K_X = K_{\langle \chi \rangle}$.

Observación 9.4.36. Con las notaciones anteriores, tenemos que H es subgrupo de G_M y que $G_M/H \cong \text{Gal}(K_X/K)$. Por la Proposición 6.1.11, $H^\perp \cong (\widehat{G_M/H}) \cong \text{Gal}(\widehat{K_X}/K)$. Puesto que G_M es abeliano, $H^\perp \cong \text{Gal}(K_X/K)$.

También, si $\chi \in X < \widehat{G_M}$, puesto que $\text{núc } \chi \supseteq H$, podemos considerar el mapeo inducido $\tilde{\chi}: G_M/H \rightarrow \mathbb{C}^*$. Por lo tanto $X \subseteq \widehat{G_M/H} \cong H^\perp$. Ahora $X^\perp < G_M$ y si $\alpha \in X^\perp$, entonces $\chi(\alpha) = 1$ para toda $\chi \in X$. Por tanto $\alpha \in H$ y $X^\perp \subseteq H$ de tal forma que $H^\perp \subseteq X^{\perp\perp} = X$. Se sigue que

$$X = H^\perp \cong \text{Gal}(\widehat{K_X}/K) \cong \text{Gal}(K_X/K).$$

Sea X un grupo finito de caracteres de Dirichlet. Puesto que $X \cong \text{Gal}(\widehat{K_X}/K)$, podemos considerar el apareamiento natural

$$\begin{aligned}\Psi: \text{Gal}(K_X/K) \times X &\longrightarrow \mathbb{C}^* \\ (g, \chi) &\longmapsto \chi(g).\end{aligned}$$

Bajo Ψ tenemos que si L es un subcampo de K_X , sea

$$Y_L = \text{Gal}(K_X/L)^\perp \cong \left(\frac{\widehat{\text{Gal}(K_X/K)}}{\widehat{\text{Gal}(K_X/L)}} \right) \cong \widehat{\text{Gal}(L/K)}.$$

Recíprocamente, si $Y \subseteq X$ es un subgrupo de X , sea $L_Y = K_X^{Y^\perp}$. Entonces L_Y es el campo fijo de $\{g \in \text{Gal}(K_X/K) \mid \chi(g) = 1 \ \forall \ \chi \in Y\}$. Se tiene $Y^\perp = \text{Gal}(K_X/L_Y)$, así que $Y = Y^{\perp\perp} = \text{Gal}(K_X/L_Y)^\perp = Y_{L_Y}$.

Por otro lado, $L_{Y_L} = K_X^{Y_L^\perp} = K_X^{(\text{Gal}(K_X/L)^\perp)^\perp} = K_X^{\text{Gal}(K_X/L)} = L$. En otras palabras hemos probado:

Teorema 9.4.37. *Existe una correspondencia biyectiva entre $\mathcal{A} = \{Y \mid Y < X\}$ y $\mathcal{B} = \{L \mid L \subseteq K_X\}$ dada por*

$$\begin{aligned}\mathcal{A} &\longleftrightarrow \mathcal{B} \\ Y &\longrightarrow L_Y = K_X^{Y^\perp} \\ \widehat{\text{Gal}(L/K)} &\cong \widehat{\text{Gal}(K_X/L)}^\perp = Y_L \longleftarrow L\end{aligned}$$

En particular obtenemos una correspondencia uno a uno entre todos los subgrupos de caracteres de Dirichlet y subcampos de campos de funciones ciclotómicos. \square

Observación 9.4.38. Puesto que $\text{Gal}(L/K)$ es un grupo finito, tenemos que $\text{Gal}(L/K) \cong \widehat{\widehat{\text{Gal}(L/K)}} \cong Y_L$. Esto se puede expresar por medio del pareo natural no degenerado

$$\begin{aligned}\text{Gal}(L/K) \times Y_L &\longrightarrow \mathbb{C}^* \\ (g, \chi) &\longmapsto \chi(g).\end{aligned}$$

Similar a la Proposición 6.2.41, tenemos

Proposición 9.4.39. *Sean X_1, X_2 dos grupos de caracteres de Dirichlet y sean $K_i = K_{X_i}$, $i = 1, 2$, los campos pertenecientes a cada X_i . Entonces*

- (1) $X_1 \subseteq X_2$ si y solamente si $K_1 \subseteq K_2$.
- (2) $K_{\langle X_1, X_2 \rangle} = K_1 K_2$.

\square

9.5. Caracteres de Dirichlet y aritmética de campos de funciones ciclotómicas

En esta sección veremos que los caracteres de Dirichlet pueden ser aplicados para estudiar algunas propiedades aritméticas de campos de funciones ciclotómicas.

Sea $M \in R_T \setminus \{0\}$ mónico y sea $M = \prod_{i=1}^r P_i^{\alpha_i}$ su descomposición como producto de polinomios irreducibles. Entonces

$$(R_T/\langle M \rangle)^* \cong \prod_{i=1}^r (R_T/\langle P_i^{\alpha_i} \rangle)^* \quad (9.6)$$

con isomorfismo φ .

Si χ es un caracter de Dirichlet módulo M , entonces correspondiente a (9.6) se tiene $\chi = \prod_{i=1}^r \chi_{P_i}$ en donde χ_{P_i} es un caracter módulo $P_i^{\alpha_i}$. En otras palabras

$$\chi(A \bmod M) = \prod_{i=1}^r \chi_{P_i}(A \bmod P_i^{\alpha_i}).$$

Se tiene $\chi_{P_i} = \chi \circ \varphi^{-1} \circ g_{P_i}$ donde $g_{P_i}: (R_T/\langle P_i^{\alpha_i} \rangle)^* \rightarrow \prod_{j=1}^r (R_T/\langle P_j^{\alpha_j} \rangle)^*$ está dado por $g_{P_i}(A) = (1, \dots, 1, A, 1, \dots, 1)$.

Ejemplo 9.5.1. Sea χ y φ como en el Ejemplo 9.4.19. Entonces χ está definido módulo $T^2(T^2 + 1)$ y φ definido módulo T^2 . Sea $\phi := \chi\varphi$, donde ϕ está definido módulo $T^2 + 1$. Tenemos $\chi = (\chi\varphi)\varphi^{-1} = \phi\varphi^{-1}$ y ϕ está definido $T^2 + 1$ de tal forma que $\chi_{T^2} = \varphi^{-1} = \varphi$ y $\chi_{T^2+1} = \phi$.

Definición 9.5.2. Sea X un grupo finito de caracteres. Entonces por un polinomio mónico e irreducible $P \in R_T$ definimos: $X_P = \{\chi_P \mid \chi \in X\}$.

Ejemplo 9.5.3. Sea $q = 2$. Consideremos $M = T^2N$ con $N = T^2 + T + 1$ y $\theta: (R_T/\langle M \rangle)^* \rightarrow \mathbb{C}^*$ donde

$$\begin{aligned} \theta(1) &= 1, & \theta(T+1) &= \zeta, & \theta(T^2+1) &= \zeta^2, & \theta(T^3+T^2+T+1) &= -1, \\ \theta(T^3+T^2+1) &= -\zeta, & \theta(T^3+T+1) &= -\zeta^2 & \text{donde } \zeta &= \zeta_6 = e^{2\pi i/6}. \end{aligned}$$

Tenemos $\theta = \theta_{P_1}\theta_{P_2}$ donde $P_1 = T$ y $P_2 = N$,

$$\begin{aligned} \theta_{P_1}: (R_T/\langle T^2 \rangle)^* &\longrightarrow \mathbb{C}^*, & \theta_{P_2}: (R_T/\langle N \rangle)^* &\longrightarrow \mathbb{C}^*, \\ \varphi^{-1} \circ g_{P_1}: (R_T/\langle T^2 \rangle)^* &\longrightarrow (R_T/\langle M \rangle)^* & \text{con} \\ 1 &\mapsto (1, 1) \mapsto 1, & T+1 &\mapsto (T+1, 1) = \\ &= (T^3+T^2+T+1, T^3+T^2+T+1) & \mapsto T^3+T^2+T+1 \end{aligned}$$

pues $T^3+T^2+T+1 \equiv T+1 \bmod T^2$, $T^3+T^2+T+1 \equiv 1 \bmod N$ y

$$\begin{aligned}
 & \varphi^{-1} \circ g_{P_2}: (R_T/\langle N \rangle)^* \rightarrow (R_T/\langle M \rangle)^* \quad \text{con} \\
 & 1 \mapsto (1, 1) \mapsto 1, \quad T \mapsto (1, T) = (T^2 + 1, T^2 + 1) \mapsto T^2 + 1, \\
 & T + 1 \mapsto (1, T + 1) = (T^3 + T^2 + 1, T^3 + T^2 + 1) \mapsto T^3 + T^2 + 1 \quad \text{pues} \\
 & T^2 + 1 \equiv 1 \pmod{T^2}, \quad T^2 + 1 \equiv T \pmod{N}, \quad T^3 + T^2 + 1 \equiv 1 \pmod{T^2} \quad \text{y} \\
 & T^3 + T^2 + 1 \equiv T + 1 \pmod{N}.
 \end{aligned}$$

Luego $\theta_{P_1} = \theta \circ \varphi^{-1} g_{P_1}$, $\theta_{P_2} = \theta \circ \varphi^{-1} g_{P_2}$,

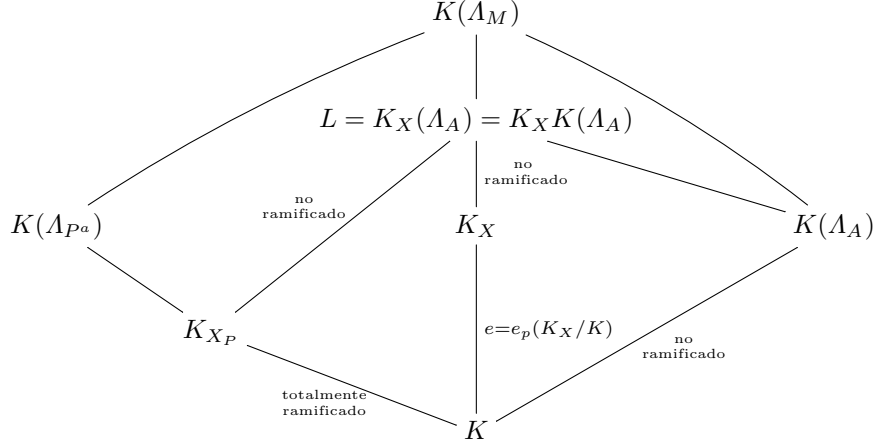
$$\begin{aligned}
 \theta_{P_1}(1) &= 1, \quad \theta_{P_1}(T + 1) = \theta(T^3 + T^2 + T + 1) = -1, \\
 \theta_{P_2}(1) &= 1, \quad \theta_{P_2}(T) = \theta(T^2 + 1) = \omega, \quad \theta_{P_2}(T + 1) = \theta(T^3 + T^2 + 1) = \omega^2,
 \end{aligned}$$

donde $\omega = \zeta^2 = e^{2\pi i/3}$.

Si $X = \langle \theta \rangle$, entonces $X_{P_1} = \langle \theta_{P_1} \rangle$, $X_{P_2} = \langle \theta_{P_2} \rangle$, y $X_P = \{1\}$ si $P \notin \{T, N\}$.

Teorema 9.5.4. Sean X un grupo finito de caracteres de Dirichlet y K_X su campo asociado. Sea $P \in R_T \setminus \{0\}$ un polinomio irreducible y sea $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{g_P}}$. Sea \mathfrak{P} un divisor primo de K_X sobre \mathfrak{p} y sea $e := e(\mathfrak{P}|\mathfrak{p})$. Entonces $e = |X_P|$.

Demostración. Sea M el mínimo común múltiplo de $\{F_\chi \mid \chi \in X\}$. Entonces $K_X \subseteq K(\Lambda_M)$. Sea $M = P^a A$ donde $A \in R_T$ y P no divide a A . Sea $L = K_X(\Lambda_A) = K_X K(\Lambda_A)$. Consideremos el siguiente diagrama donde la ramificación se refiere a P .



Entonces por la Proposición 9.4.39 se tiene $L = K_X K(\Lambda_A) = K_X K_{\widehat{G_A}} = K_{\widehat{\langle X, G_A \rangle}}$.

Así que L es el campo perteneciente al grupo generado por X y $\widehat{G_A}$, esto es, el grupo de caracteres de L está generado por X y por los caracteres de Dirichlet de G_M cuyo conductor es primo relativo a P .

Como en la demostración del Teorema 6.3.3 se tiene que $\langle X, \widehat{G_A} \rangle \cong X_P \times \widehat{G_A}$.

Ahora bien $K_{X_P} \subseteq K(\Lambda_{P^a})$ y $L = K_{X_P}K(\Lambda_A)$. Se tiene que \mathfrak{p} es no ramificado en $K(\Lambda_A)/K$ y por tanto el índice de ramificación de \mathfrak{p} en K_X/K es el mismo que el de L/K . Por otro lado, puesto que L/K_{X_P} no es ramificado en los divisores primos que están sobre \mathfrak{p} y por el Teorema 9.2.25 (4), \mathfrak{p} es totalmente ramificado en K_{X_P}/K , concluimos que $e = [K_{X_P} : K] = |X_P|$. \square

Ejemplo 9.5.5. En el Ejemplo 9.5.3, el índice de ramificación de $P_1 = T$ es $|X_{P_1}| = 2$ pues $X_{P_1} = \langle \theta_{P_1} \rangle$ y θ_{P_1} es de orden 2 y el índice de ramificación de $P_2 = T^2 + T + 1$ es $|X_{P_2}| = 3$ pues $X_{P_2} = \langle \theta_{P_2} \rangle$ y θ_{P_2} es de orden 3. Finalmente para otro primo distinto a P_1 , P_2 y \mathfrak{p}_∞ se tiene que el índice de ramificación es 1, es decir, es no ramificado.

Ejemplo 9.5.6. Sea $q = 2$ y consideremos el caracter χ dado en el Ejemplo 9.4.19. El conductor de χ es $T^2(T^2 + 1)$. Por el Ejemplo 9.5.1 tenemos que $\chi_{T^2} = \varphi$ y $\chi_{T^2+1} = \phi$. Notemos que $\Phi(T^2) = \Phi(T^2 + 1) = q^{dn} - q^{d(n-1)} = 2^{1(2)} - 2^{1(2-1)} = 2^2 - 2 = 4 - 2 = 2$. De aquí que $[K(\Lambda_{T^2}) : K] = [K(\Lambda_{T^2+1}) : K] = 2$. Tenemos

$$u^{T^2} = \sum_{i=0}^2 \begin{bmatrix} T^2 \\ i \end{bmatrix} u^{q^i} = T^2 u + \begin{bmatrix} T^2 \\ 1 \end{bmatrix} u^q + uq^2.$$

Ahora bien,

$$\begin{bmatrix} T^2 \\ 1 \end{bmatrix} = T \begin{bmatrix} T \\ 1 \end{bmatrix} + \begin{bmatrix} T \\ 0 \end{bmatrix}^q = T + T^q = T + T^2$$

donde $\begin{bmatrix} T \\ 1 \end{bmatrix} = a_1 = 1$. Por lo tanto

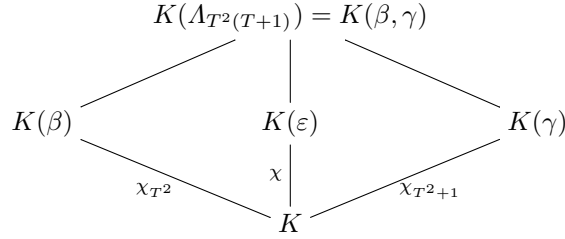
$$u^{T^2} = T^2 + (T + T^2)u^2 + u^4.$$

También tenemos

$$\Psi_{T^2}(u) = \frac{u^{T^2}}{u^T} = \frac{T^2 u + (T + T^2)u^2 + u^4}{Tu + u^2} = u^2 + Tu + T.$$

Por lo tanto cada raíz α de $\Psi_{T^2}(u)$ es de la forma: $(\frac{\alpha}{T})^2 + (\frac{\alpha}{T}) = -\frac{1}{T} = \frac{1}{T}$. Por lo tanto $K(\Lambda_{T^2}) = K(\beta)$ donde β es una raíz de la extensión de Artin-Schreier que satisface $\beta^2 - \beta = \frac{1}{T}$.

Similarmente, $K(\Lambda_{T^2+1}) = K(\gamma)$ donde $\gamma^2 + \gamma = \frac{1}{T+1}$. Se sigue que $K_\chi = K(\varepsilon)$ con $\varepsilon^2 - \varepsilon = \frac{1}{T(T+1)}$ y tenemos el siguiente diagrama



En $K(\varepsilon)/K$, T y $T+1$ son los primos ramificados. En $K(\beta)/K$, T es el único primo ramificado y en $K(\gamma)/K$, $T+1$ es el único primo ramificado.

Corolario 9.5.7. Sea χ un caracter de Dirichlet. Entonces P se ramifica en K_χ/K si y sólo si $\chi(P) = 0$, o equivalentemente, P divide a F_χ . Si X es cualquier grupo finito de caracteres de Dirichlet, entonces P es no ramificado en K_X/K si y sólo si $\chi(P) \neq 0$ para toda $\chi \in X$.

Demostración. Se tienen las equivalencias: P es ramificado en $K_X/K \iff X_P \neq \{1\} \iff$ existe $\chi \in X$ tal que $\chi_P \neq 1 \iff$ existe $\chi \in X$ con $P|F_\chi \iff$ existe $\chi \in X$ con $\chi(P) = 0$. \square

Como en el caso numérico, Teorema 6.3.5, los grupos de inercia y de descomposición están relacionados con los caracteres de Dirichlet de la siguiente manera.

Teorema 9.5.8. Sea X un grupo finito de caracteres de Dirichlet y sea K_X su campo asociado. Sean $P \in R_T$ y $Y = \{\chi \in X \mid \chi(P) \neq 0\}$, $Z = \{\chi \in X \mid \chi(P) = 1\}$. Entonces, si $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_{\infty}^{\text{gr } P}}$, consideremos \mathfrak{P} un divisor primo en K_X sobre \mathfrak{p} . Entonces

$$X/Y \cong \widehat{I(\mathfrak{P}|\mathfrak{p})} \cong I(\mathfrak{P}|\mathfrak{p}) \quad \text{y} \quad X/Z \cong D(\mathfrak{P}|\mathfrak{p}).$$

En particular, $e = e(\mathfrak{P}|\mathfrak{p}) = [X : Y]$, $f = d(\mathfrak{P}|\mathfrak{p}) = [Y : Z]$ y $h = [Z : 1] = |Z|$ donde h es el número de divisores primos en K_X sobre \mathfrak{p} . Finalmente, el grupo Y/Z es cíclico de orden f .

Demostración. Análoga a la del Teorema 6.3.5. \square

Resolveremos el problema inverso de la Teoría de Galois para el caso particular de un grupo abeliano. Primero necesitamos el siguiente resultado.

Proposición 9.5.9. Sea $P \in R_T$ un polinomio irreducible mónico de grado d y sea $n = p^t$. Entonces $(R_T/\langle P^n \rangle)^*$ contiene un subgrupo cíclico de orden $p^t a$ para cualquier a que divide a $q^d - 1$.

Demostración. Se tiene que $|(R_T/\langle P^n \rangle)^*| = \Phi(P^n) = q^{dn} - q^{d(n-1)} = q^{d(n-1)}(q^d - 1)$.

Por tanto $(R_T/\langle P^n \rangle)^*$ es isomorfo a una suma directa $H \oplus A$ donde $|H| = q^{d(n-1)}$ y $|A| = q^d - 1$. Notemos que A es el único subgrupo de orden $q^d - 1$. Definimos

$$\begin{aligned} \theta: (R_T/\langle P^n \rangle)^* &\longrightarrow (R_T/\langle P \rangle)^* \\ B \text{ mód } P^n &\longmapsto B \text{ mód } P. \end{aligned}$$

Entonces θ es un epimorfismo y $(R_T/\langle P^n \rangle)^* / \text{núc } \theta \cong (R_T/\langle P \rangle)^*$.

Puesto que $|(R_T/\langle P \rangle)^*| = \Phi(P) = q^d - 1$, se sigue que

$$A \cong (R_T/\langle P \rangle)^* \quad \text{y} \quad H \cong \text{núc } \theta \cong \{B \text{ mód } P^n \mid B \equiv 1 \text{ mód } P\}.$$

Ahora $R_T/\langle P \rangle$ y \mathbb{F}_{q^d} son isomorfos de tal forma que A es el grupo multiplicativo de los elementos diferentes de cero de un campo y por lo tanto A es un grupo cíclico.

Sea $B = 1 + P$. Queremos determinar el orden de B módulo P^n en $R_T/\langle P^n \rangle$. Ahora como $B \in \text{núc } \theta$, $B \in H$, y $o(B) = p^s$ para algún $s \geq 0$. Entonces

$$B^{p^s} = 1 + P^{p^s} \equiv 1 \text{ mód } P^n \iff p^s \geq n = p^t \iff s \geq t.$$

Por tanto $o(B) = p^t$. □

Teorema 9.5.10. *Sea G un grupo abeliano finito. Entonces existen campos de funciones congruentes E y F tales que*

- (I) $\text{Gal}(F/E) \cong G$.
- (II) F/E es no ramificada en todos los divisores primos.
- (III) F/K es abeliana y E/K es cíclica.
- (IV) El campo de constantes, tanto de E como de F es \mathbb{F}_q .

Demostración. Sea $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$. Definimos $m_i = p^{t_i}a_i$ con $\text{mcd}(a_i, p) = 1$, $t_i \geq 0$ para $1 \leq i \leq r$. Sea $d'_i = o(p \text{ mód } a_i)$, es decir, $p^{d'_i} \equiv 1 \text{ mód } a_i$, con d'_i mínimo. Escojamos números naturales $d_1 < d_2 < \cdots < d_r$ donde cada d'_i divide a d_i . Por ejemplo, podemos tomar $d_1 = d'_1$, $d_i = 2d_{i-1}d'_i$, $i = 2, \dots, r$. Sea $P_i \in R_T$ un polinomio mónico irreducible de grado d_i . Tal polinomio P_i existe pues si $\mathbb{F}_{q^{d_i}} = \mathbb{F}_q(\alpha_i)$ para algún α_i , entonces $P_i = \text{Irr}(\alpha_i, T, \mathbb{F}_q)$ es de grado d_i y $\mathbb{F}(\alpha_i) \cong R_T/\langle P_i \rangle$.

Por la Proposición 9.5.9, $(R_T/\langle P_i^{p^{t_i}} \rangle)^*$ contiene un elemento de orden $p^{t_i}a_i = m_i$. Ahora, puesto que $(R_T/\langle P_i^{p^{t_i}} \rangle)^* \cong (R_T/\langle P_i^{p^{t_i}} \rangle)^*$, existe un carácter χ mód $P_i^{t_i}$ de orden m_i . Es decir χ satisface $o(\chi) = m_i$ y $F_{\chi_i} = p_i^{s_i}$ con $s_i \leq t_i$.

Sea P_{r+1} otro polinomio mónico irreducible de grado $d_{r+1} > d_r$ tal que $a_1 \cdots a_r | q^{d_{r+1}} - 1$. Tal d_{r+1} existe pues $\text{mcd}(a_1 \cdots a_r, q) = 1$.

Sea χ_{r+1} un caracter de Dirichlet definido módulo $P_{r+1}^{p^t}$ para $t = t_1 + \dots + t_r$ y orden $m_{r+1} = p^t(q^{d_{r+1}} - 1)$ (Proposición 9.5.9). Entonces

$$m_1 \cdots m_r = a_1 \cdots a_r p^{t_1 + \dots + t_r} |m_{r+1}.$$

Sea $\chi := \chi_1 \cdots \chi_r \chi_{r+1}$ y $E := K_X$ el campo asociado a $X := \langle \chi \rangle$. Sea $Y := \langle \chi_1, \dots, \chi_r, \chi_{r+1} \rangle$ y $F := K_Y$ el campo correspondiente a Y . Tenemos

$$K \subseteq E = K_X \subseteq K_Y = F \subseteq K(\Lambda_M)$$

donde $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r} P_{r+1}^{\alpha_{r+1}}$ con $\alpha_i = p^{t_i}$, $1 \leq i \leq r$ y $\alpha_{r+1} = p^t$. En particular el campo de constantes de E y F es \mathbb{F}_q (Corolario 9.2.26). Esto prueba (iv) y también tenemos que F/K es una extensión abeliana.

Por otro lado se tiene $\text{Gal}(E/K) \cong X \cong \langle \chi \rangle$ es cíclico y obtenemos (III). Ahora bien, $Y = \langle \chi_1, \dots, \chi_r, \chi_{r+1} \rangle = \langle \chi_1, \dots, \chi_r, \chi \rangle$ y $o(\chi) = o(\chi_{r+1}) = m_{r+1}$ y puesto que $m_1 \cdots m_r$ divide a m_{r+1} , χ es de orden maximal en Y .

Por tanto $Y/X = Y/\langle \chi \rangle \cong \langle \chi_1, \dots, \chi_r \rangle$ y

$$\begin{aligned} Y/X &\cong \frac{\widehat{\text{Gal}(K_Y/K)}}{\widehat{\text{Gal}(K_X/K)}} \cong \frac{\widehat{\text{Gal}(K_Y/K)}}{\left(\frac{\widehat{\text{Gal}(K_Y/K)}}{\widehat{\text{Gal}(K_Y/K_X)}} \right)} \cong \widehat{\text{Gal}(K_Y/K_X)} \\ &\cong \widehat{\text{Gal}(F/E)} \cong \text{Gal}(F/E). \end{aligned}$$

Se obtiene que $\text{Gal}(F/E) \cong \langle \chi_1, \dots, \chi_r \rangle \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \cong G$ lo cual prueba (I).

Por el Teorema 9.3.5 se tiene que los primos ramificados en F/K son $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{p}_{r+1}$ y \mathfrak{p}_∞ , donde $(P_i)_K = \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{r_i P_i}}$.

Ahora bien el índice de ramificación de \mathfrak{p}_∞ en E/K es $q-1$ lo mismo que en F/K puesto que E es el campo perteneciente a χ , $q-1|o(\chi)$ y $(R_T/\langle P_{r+1}^{p^t} \rangle)^*$ contiene un único subgrupo de orden $(q-1)$ (Proposición 9.5.9) y este grupo es el grupo de inercia \mathfrak{p}_∞ (Teorema 9.2.27). Por lo tanto \mathfrak{p}_∞ es no ramificado en F/E . Finalmente tenemos $Y_{P_i} = \langle \chi_i \rangle = X_{P_i}$. Por el Teorema 9.5.4 se tiene que índice de ramificación en cada divisor en F que divide a \mathfrak{p}_i es $\frac{|Y_{P_i}|}{|X_{P_i}|} = 1$.

Por tanto F/E es no ramificada en cada divisor primo y esto prueba (II) y el teorema. \square

Definición 9.5.11. Sea $P \in R_T$ un polinomio mónico e irreducible de grado d . Entonces $R_T/\langle P \rangle$ es el campo de q^d elementos. Si $Q \in R_T$ es mónico e irreducible, $Q \neq P$, $Q \bmod P \in \mathbb{F}_{q^d}^*$ y en particular $Q^{q^d-1} \bmod P \equiv 1 \bmod P$.

Se define el símbolo de Legendre $\left(\frac{Q}{P}\right) = \left(\frac{Q}{P}\right)_{q-1}$ como el único elemento

$\alpha \in \mathbb{F}_{q^d}^*$ tal que $Q^{\frac{q^d-1}{q-1}} \bmod P = \alpha$.

Ejemplo 9.5.12. Sea P un polinomio irreducible de grado d . Se tiene que $K(\Lambda_P)/K$ es una extensión cíclica de grado $q^d - 1$. Por tanto existe un único subcampo de $K(\Lambda_P)$ de grado $q - 1$ sobre K : $[L : K] = q - 1$. Ahora bien, puesto que $\mathbb{F}_q^* \subseteq K$, se tiene que las $q - 1$ raíces de unidad están en K y por tanto L/K es una extensión de Kummer. Sea $L = K(\alpha)$ donde $\alpha^{q-1} = \beta \in K$. Ahora puesto que los primos ramificados en L/K son \mathfrak{p} y \mathfrak{p}_∞ , donde $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^P}$ y son totalmente ramificados como consecuencia de los Teoremas 9.2.25 y 9.2.27, se tiene $\beta \in R_T$ y $\beta = \gamma P^i$ con $\gamma \in \mathbb{F}_q^*$ y $\text{mcd}(i, q - 1) = 1$.

Por Teoría de Kummer, podemos tomar $i = 1$ y se tiene $\alpha^{q-1} = \gamma P$. Si ζ es un generador de \mathbb{F}_q^* , equivalentemente, ζ es una $q - 1$ raíz primitiva de 1, se tiene que si $G = \text{Gal}(L/K)$, entonces $\sigma\alpha = \zeta\alpha$ para algún generador σ de G : $G = \langle \sigma \rangle$.

Proposición 9.5.13. Para $P \in R_T^+$, $K(\sqrt[q]{(-1)^d P}) \subseteq K(\Lambda_P)$, donde l es cualquier divisor de $q - 1$.

Demostración. Sea $\Phi_P(u) = \frac{u^P}{u}$ el P -ésimo polinomio ciclotómico. Tenemos

$$\Phi_P(u) = \prod_{\substack{A \neq 0, A \in R_T \\ \text{gr } A < \text{gr } P}} (u - \lambda^A) = \sum_{i=0}^d \binom{P}{i} u^{q^i - 1},$$

donde $\lambda \in \Lambda_P \setminus \{0\}$, esto es, λ es un generador como R_T -módulo de Λ_P . Entonces

$$\Phi_P(0) = (-1)^{q^d - 1} \prod_{\substack{A \neq 0, A \in R_T \\ \text{gr } A < \text{gr } P}} \lambda^A = P.$$

Ahora, todo polinomio $A \in R_T$, $A \neq 0$ puede ser unívocamente escrito como producto de un elemento $\alpha \in \mathbb{F}_q^*$ y un polinomio mónico A_1 : $A = \alpha A_1$. Ahora, $\lambda^A = \lambda^{\alpha A_1} = \alpha \lambda^{A_1}$. Notemos que hay exactamente $q - 1$ polinomios $A \in R_T$, $A \neq 0$ tal que A_1 aparece, una para cada uno de los $q - 1$ elementos de \mathbb{F}_q^* . Por lo tanto

$$\begin{aligned} P &= (-1)^{q^d - 1} \prod_{\substack{A \neq 0, A \in R_T \\ \text{gr } A < \text{gr } P}} \lambda^A = (-1)^{q^d - 1} \prod_{\substack{A_1 \text{ mónico} \\ \alpha \in \mathbb{F}_q^*}} \alpha \lambda^{A_1} \\ &= (-1)^{q^d - 1} \left(\prod_{\alpha \in \mathbb{F}_q^*} \alpha \right)^{\frac{q^d - 1}{q - 1}} \left(\prod_{A_1 \text{ mónico}} \lambda^{A_1} \right)^{q - 1}. \end{aligned}$$

Notemos que $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$ lo cual se sigue de que $\frac{x^q - x}{x} = x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^*} (x - \alpha)$ por lo que $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$, y que $\xi := \prod_{A_1 \text{ mónico}} \lambda^{A_1} \in K(\Lambda_P)$.

Entonces

$$(-1)^{q^d - 1} (-1)^{(q^d - 1)/(q - 1)} \xi^{q - 1} = (-1)^d \xi^{q - 1} = P,$$

con $\xi \in K(\Lambda_P)$. Se sigue que $\xi = \sqrt[q-1]{(-1)^d P} \in K(\Lambda_P)$. En particular $\sqrt[l]{(-1)^d P} = \xi^{(q-1)/l} \in K(\Lambda_P)$. \square

Corolario 9.5.14. *Sea $D \in R_T$ un polinomio mónico. Entonces*

$$K(\sqrt[l]{(-1)^{\text{gr } D} D}) \subseteq K(\Lambda_D),$$

donde l es cualquier divisor de $q-1$. \square

Así, tenemos $L = K(\sqrt[q-1]{(-1)^d P})$ con $d = \text{gr } P$. Sea $\theta: (R_T/\langle P \rangle)^* \rightarrow \mathbb{C}^*$ el caracter asociado a K . Puesto que $X = \langle \theta \rangle$ es de orden $|X| = q-1$, se tiene $\theta^{q-1} = 1$, $\theta \neq \text{Id}$, $F_\theta = P$ y $\theta((R_T/\langle P \rangle)^*) = \{\zeta \in \mathbb{C}^* \mid \zeta^{q-1} = 1\}$.

Se tiene que $L = K(\Lambda_P)^{\text{nuc } \theta}$, $\text{nuc } \theta = \{\sigma \in G_P \mid \theta(\sigma) = 1\}$. Sea Q un polinomio irreducible tal que $Q \neq P$. Se tiene que Q se descompone totalmente en L/K si y sólo si $Z = \{\chi \in X \mid \chi(Q) = 1\}$ satisface que $|Z| = q-1$, es decir si y sólo si $Z = X$. Se sigue que Q se descompone totalmente en L/K si y sólo si $\theta(Q) = 1$.

El símbolo de Legendre $\left(\frac{Q}{P}\right) = \left(\frac{Q}{P}\right)_{q-1}$ satisface que $\left(\frac{Q}{P}\right)$ es el único elemento \mathbb{F}_q^* tal que

$$\left(\frac{Q}{P}\right) = Q^{\frac{q^d-1}{q-1}} \text{ mód } P.$$

Ahora si $Q = B^{q-1} \text{ mód } P$ para algún B , se tiene que $\theta(Q) = \theta(B^{q-1}) = (\theta(B))^{q-1}$ lo cual implica que $Q \in \text{nuc } \theta$. Puesto que

$$|\text{nuc } \theta| = \frac{|(R_T/\langle P \rangle)^*|}{q-1} = \frac{q^d-1}{q-1} = \left| \left((R_T/\langle P \rangle)^* \right)^{q-1} \right|,$$

se sigue que $\text{nuc } \theta \left((R_T/\langle P \rangle)^* \right)^{q-1}$, y por tanto $\theta(Q) = 1$ si y sólo si $Q \equiv B^{q-1} \text{ mód } P$ si y sólo si $\left(\frac{Q}{P}\right) = 1$ y en particular $\text{nuc } \theta = \left\{ Q \mid \left(\frac{Q}{P}\right) = 1 \right\} = \text{nuc } \left(\frac{Q}{P}\right)$.

En resumen $L = K(\sqrt[q-1]{(-1)^d P})$ es el campo asociado a $\left(\frac{Q}{P}\right)$.

9.6. Fórmula del conductor–discriminante

Primero calculemos el diferente de una extensión ciclotómica $K(\Lambda_M)/K$.

Proposición 9.6.1. *Sea $P \in R_T$ un polinomio mónico e irreducible de grado d y sea $n \in \mathbb{N}$. Si $M = P^n$, entonces el diferente de $K(\Lambda_{P^n})/K$ \mathfrak{D}_{P^n} está dado por:*

$$\mathfrak{D}_{P^n} = \mathfrak{P}^s \prod_{\mathfrak{Q}|\mathfrak{p}_\infty} \mathfrak{Q}^{q-2}$$

donde \mathfrak{P} es único divisor primo sobre \mathfrak{p} ,

$$\begin{aligned} s &= n\Phi(P^n) - q^{d(n-1)} = nq^{dn} - (n+1)q^{d(n-1)} \quad y \\ 2g_{P^n} - 2 &= (dq n - dn - q) \frac{\Phi(P^n)}{q-1} - dq^{d(n-1)}, \end{aligned}$$

donde g_{P^n} denota al género de $K(\Lambda_{P^n})$.

Demostración. Por los Teoremas 9.2.25 y 9.2.27 se tiene que cualquier divisor primo diferente a \mathfrak{p} y \mathfrak{p}_∞ es no ramificado en $K(\Lambda_{P^n})/K$, \mathfrak{p} es totalmente ramificado y \mathfrak{p}_∞ es moderadamente ramificado. Se sigue que $\mathfrak{D}_{P^n} = \mathfrak{P}^s \prod_{\mathfrak{Q}|\mathfrak{p}_\infty} \mathfrak{Q}^{q-2}$.

Solo falta determinar s . Se tiene que $\mathcal{O}_{P^n} = R_T[\lambda]$ donde λ es raíz de $\Psi_{P^n}(u)$ y $s = v_{\mathfrak{P}}(\Psi_{P^n}(\lambda))$. Ahora bien, puesto que $u^{P^n} = u^{P^{n-1}}\Psi_{P^n}(u)$ se sigue que

$$\begin{aligned} P^n &= (u^{P^n})' = (u^{P^{n-1}})' \Psi_{P^n}(u) + u^{P^{n-1}} \Psi'_{P^n}(u) = \\ &= P^{n-1} \Psi_{P^n}(u) + u^{P^{n-1}} \Psi'_{P^n}(u). \end{aligned}$$

Por lo tanto $P^n = \lambda^{P^{n-1}} \Psi'_{P^n}(\lambda)$ y $(\Psi'_{P^n}(\lambda)) = (\frac{P^n}{\lambda^{P^{n-1}}})$.

Puesto que $\lambda^{P^{n-1}} \in \Lambda_P$ y $\Psi_P(u) = \prod_{\text{mcd}(A,P)=1} (u - \lambda_P^A)$, se tiene

$$\Psi_P(0) = P = \pm \prod_{\text{mcd}(S,P)=1} \lambda_P^S = \alpha \lambda_P^{\Phi(P)}$$

donde α es una unidad de \mathcal{O}_{P^n} . En particular tenemos que $\langle (\lambda^{P^{n-1}})^{\Phi(P)} \rangle = \langle P \rangle$. Si \mathfrak{q} es el único divisor primo de $K(\Lambda_P)$ que divide a \mathfrak{p} , entonces $v_{\mathfrak{q}}(\lambda^{P^{n-1}}) = \frac{v_{\mathfrak{q}}(P)}{\Phi(P)} = \frac{e(\mathfrak{q}|\mathfrak{p})v_{\mathfrak{p}}(P)}{\Phi(P)} = 1$ pues $\mathfrak{q}|\mathfrak{p}$ es totalmente ramificado en $K(\Lambda_P)/K$. Entonces

$$v_{\mathfrak{P}}(\lambda^{P^{n-1}}) = e(\mathfrak{p}|\mathfrak{q})v_{\mathfrak{q}}(\lambda^{P^{n-1}}) = \frac{\Phi(P^n)}{\Phi(P)}.$$

Se sigue que $s = v_{\mathfrak{P}}(\Psi'_{P^n}(\lambda)) = v_{\mathfrak{P}}(\frac{P^n}{\lambda^{P^{n-1}}}) = n\Phi(P^n) - q^{d(n-1)}$. Por la fórmula del género de Riemann–Hurwitz (Teorema 8.6.5) obtenemos

$$\begin{aligned}
 2g_{K(\Lambda_{P^n})} - 2 &= [K(\Lambda_{P^n}) : K](2g_K - 2) + d_{K(\Lambda_{P^n})}(\mathfrak{D}_{P^n}) \\
 &= \Phi(P^n)(0 - 2) + d(n\Phi(P^n) - q^{d(n-1)}) + \frac{\Phi(P^n)}{q-1}(q-2) \\
 &= \frac{\Phi(P^n)}{(q-1)}(-2(q-1) + dn(q-1) + (q-2)) - dq^{d(n-1)} \\
 &= (dnq - dn - 2q + 2 - q - 2)\frac{\Phi(P^n)}{q-1} - dq^{d(n-1)} \\
 &= (dq n - dn - q)\frac{\Phi(P^n)}{q-1} - dq^{d(n-1)}. \quad \square
 \end{aligned}$$

El resultado general es:

Teorema 9.6.2 (Fórmula del género y del diferente). *Sea $M \in R_T$ un polinomio mónico no constante de la forma $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ donde P_1, \dots, P_r son polinomios irreducibles distintos. Sea $d_i = \text{gr } P_i$. Entonces*

$$\mathfrak{D}_M = \prod_{i=1}^r \left(\prod_{\mathfrak{p}|\mathfrak{p}_i} \mathfrak{p} \right)^{s_i} \prod_{\mathfrak{Q}|\mathfrak{p}_\infty} \mathfrak{Q}^{q-1}$$

donde $(P_i)_K = \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{d_i}}$, $s_i = \alpha_i \Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i-1)}$ y

$$2g_M - 2 = -2\Phi(M) + \sum_{i=1}^r d_i s_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2) \frac{\Phi(M)}{q-1}.$$

Demostración. Para cada $i \in \{1, \dots, r\}$, \mathfrak{p}_i es completamente ramificado en $K(\Lambda_{P_i^{\alpha_i}})/K$ y no ramificado en $K(\Lambda_M)/K(\Lambda_{P_i^{\alpha_i}})$. Para cada divisor primo \mathfrak{q} en $K(\Lambda_{P_i^{\alpha_i}})$ que está sobre \mathfrak{p}_i , hay $\frac{\Phi(M)/\Phi(P_i^{\alpha_i})}{f_i}$ divisores primos, cada uno de ellos de grado relativo f_i . Por tanto la contribución a \mathfrak{D}_M de \mathfrak{p}_i es $\left(\prod_{\mathfrak{p}|\mathfrak{p}_i} \mathfrak{p} \right)^{s_i}$

donde s_i es como en la Proposición 9.6.1. Tenemos

$$\text{gr}_{K(\Lambda_M)} \left(\prod_{\mathfrak{p}|\mathfrak{p}_i} \mathfrak{p} \right) = d_i \frac{\Phi(M)/\Phi(P_i^{\alpha_i})}{f_i} = d_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})}.$$

Por lo tanto $\mathfrak{D}_M = \prod_{i=1}^r \left(\prod_{\mathfrak{p}|\mathfrak{p}_i} \mathfrak{p} \right)^{s_i} \prod_{\mathfrak{Q}|\mathfrak{p}_\infty} \mathfrak{Q}^{q-2}$ y

$$\begin{aligned}
 2g_M - 2 &= (2g_K - 2)[K(\Lambda_M) : K] + \text{gr}_{K(\Lambda_M)} \mathfrak{D}_M \\
 &= -2\Phi(M) + \sum_{i=1}^r s_i d_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2) \frac{\Phi(M)}{q-1}. \quad \square
 \end{aligned}$$

Veamos el siguiente ejemplo.

Ejemplo 9.6.3. Sean $q = 3$, $M = T^2(T+1)$, $\zeta = \zeta_6 = e^{2\pi i/6}$ y

$$\begin{aligned}\theta_T: (R_T/\langle T^2 \rangle)^* &\longrightarrow \mathbb{C}^* \\ 1 &\longmapsto 1 \\ T-1 &\longmapsto \zeta \\ T+1 &\longmapsto \zeta^2 \\ -1 &\longmapsto -1 \\ -T+1 &\longmapsto -\zeta \\ -T-1 &\longmapsto -\zeta^2.\end{aligned}$$

Sea $\widetilde{\theta}_T = \theta_T \circ \varphi_{M,T^2}$, y sea θ_{T+1} dado por

$$\begin{aligned}\theta_{T+1}: (R_T/\langle T+1 \rangle)^* &\longrightarrow \mathbb{C}^* \\ 1 &\longmapsto 1 \\ -1 &\longmapsto -1\end{aligned}$$

y sea $\widetilde{\theta}_{T+1} = \theta_{T+1} \circ \varphi_{M,T+1}$.

Sea $X = \langle \widetilde{\theta}_T, \widetilde{\theta}_{T+1} \rangle$. El campo perteneciente a X es $L = K(\Lambda_M)$. Tenemos $X_T = \langle \theta_T \rangle$, $X_{T+1} = \langle \theta_{T+1} \rangle$. Así, $e_T = 6$, $e_{T+1} = 2$. Notemos que los grupos Y y Z (ver Teorema 9.5.8) de T y $T+1$ satisfacen:

$$\begin{aligned}Y(T+1) &= \{\tau \in X \mid \tau(T+1) \neq 0\} = \langle \widetilde{\theta}_T \rangle \cong X_T \quad \text{y} \\ Z(T+1) &= \{\tau \in X \mid \tau(T+1) = 1\} = \langle \widetilde{\theta}_{T+1}^3 \rangle,\end{aligned}$$

luego $e_{T+1} = 2$, $f_{T+1} = 3$ y $h_{T+1} = 2$. Ahora bien

$$\begin{aligned}Y(T) &= \{\tau \in X \mid \tau(T) \neq 0\} = \langle \widetilde{\theta}_{T+1} \rangle \cong X_{T+1} \quad \text{y} \\ Z(T) &= \{\tau \in X \mid \tau(T) = 1\} = \{1\},\end{aligned}$$

luego $e_T = 6$, $f_T = 2$ y $h_T = 1$. Para \mathfrak{p}_∞ tenemos $e_\infty = 2$, $f_\infty = 1$, $h_\infty = 6$. Por tanto $s_1 = 2\Phi(T^2) - 3 = 9$, $s_2 = 1\Phi(T+1) - 3^0 = 1$, de donde el diferente de $K(\Lambda_M)/K$ es $\mathfrak{D}_M = \mathfrak{P}_T^9 \mathfrak{P}_{T+1,1} \mathfrak{P}_{T+1,2} \mathfrak{Q}_1 \mathfrak{Q}_2 \mathfrak{Q}_3 \mathfrak{Q}_4 \mathfrak{Q}_5 \mathfrak{Q}_6$. Se sigue que el diferente de \mathcal{O}_M sobre R_T es

$$\begin{aligned}\mathfrak{D}_{\mathcal{O}_M/R_T} &= \mathfrak{P}_T^p \mathfrak{P}_{T+1,1} \mathfrak{P}_{T+1,2} \quad \text{y} \\ \mathfrak{d}_{\mathcal{O}_M/R_T} &= N_{K(\Lambda_M)/K} \mathfrak{D}_{\mathcal{O}_M/R_T} = T^{18} (T+1)^6.\end{aligned}$$

Por otro lado tenemos

Caracter	Conductor
1	1
$\widetilde{\theta_T}$	T^2
$\widetilde{\theta_T^2}$	T^2
$\widetilde{\theta_T^3}$	T
$\widetilde{\theta_T^4}$	T^2
$\widetilde{\theta_T^5}$	T^2
$\widetilde{\theta_{T+1}}$	$T + 1$
$\widetilde{\theta_T \theta_{T+1}}$	$T^2(T + 1)$
$\widetilde{\theta_T^2 \theta_{T+1}}$	$T^2(T + 1)$
$\widetilde{\theta_T^3 \theta_{T+1}}$	$T(T + 1)$
$\widetilde{\theta_T^4 \theta_{T+1}}$	$T^2(T + 1)$
$\widetilde{\theta_T^5 \theta_{T+1}}$	$T^2(T + 1)$

Así

$$\begin{aligned}
 \prod_{\chi \in X} F_\chi &= 1 \cdot T^2 \cdot T^2 \cdot T \cdot T^2 \cdot T^2 \cdot (T + 1) \cdot T^2(T + 1) \cdot T^2(T + 1) \cdot \\
 &\quad \cdot T(T + 1) \cdot T^2(T + 1) \cdot T^2(T + 1) = \\
 &= T^{18}(T + 1)^6 = \mathfrak{d}_{\mathcal{O}_M/R_T}.
 \end{aligned}$$

Es decir

$$\prod_{\chi \in X} F_\chi = \mathfrak{d}_{\mathcal{O}_M/R_T}.$$

Teorema 9.6.4 (Fórmula del conductor–discriminante). *Sea L un subcampo de $K(\Lambda_M)$ donde $M \in R_T$ es un polinomio mónico no constante. Sea $\mathfrak{d}_{L/K}$ el discriminante de \mathcal{O}_L/R_T donde \mathcal{O}_L es la cerradura entera de R_T en L . Sea X_L el grupo de caracteres de Dirichlet asociado a L . Entonces*

$$\mathfrak{d}_{L/K} = \prod_{\chi \in X_L} F_\chi.$$

Demostración. La prueba se puede hacer de manera similar a la del caso numérico (Teorema 6.3.9). Aquí presentamos una demostración diferente.

Primero supongamos que $M = P^n$ donde $P \in R_T$ es un polinomio irreducible. Sean

$$L_i := L \cap K(\Lambda_{P^i}), \quad i = 0, 1, 2, \dots, n.$$

Entonces $L_0 = L$ y $L_n = K$. Tenemos que un caracter χ tiene conductor P^j si y sólo si χ es un caracter asociado al campo $K(\Lambda_{P^j})$ pero no a $K(\Lambda_{P^{j-1}})$.

Se sigue que X_L contiene exactamente $[L_j : K] - [L_{j-1} : K]$ caracteres de conductor P^j , $1 \leq j \leq n$. Por lo tanto

$$\prod_{\chi \in X_L} F_\chi = P^\alpha$$

donde

$$\alpha = \sum_{j=1}^n j([L_j : K] - [L_{j-1} : K]) = n[L_n : K] - \sum_{j=0}^{n-1} [L_j : K].$$

Por lo tanto

$$\prod_{\chi \in X_L} F_\chi = P^\alpha \quad \text{con} \quad \alpha = n[L_n : K] - \sum_{j=0}^{n-1} [L_j : K]. \quad (9.7)$$

Ahora bien, si probamos que $\mathfrak{D}_{L/K} = \mathfrak{p}_L^\alpha$ donde $\mathfrak{p}_L := \mathfrak{p}_n \cap \mathcal{O}_L$ y \mathfrak{p}_n es el único divisor primo de $K(\Lambda_{P^n})$ sobre \mathfrak{p} , puesto que el grado relativo de \mathfrak{p}_L sobre \mathfrak{p} es 1, se seguirá que

$$\mathfrak{d}_{L/K} = N_{L/K} \mathfrak{D}_{L/K} = P^\alpha.$$

Sea $\mathfrak{D}_{L/K} = \mathfrak{p}_L^\gamma$. Tenemos $\mathcal{O}_{P^n} = R_T[\lambda_{P^n}]$ y $\mathcal{O}_{P^n} = \mathcal{O}_L[\lambda_{P^n}]$. Sea $f(u) := \text{Irr}(u, \lambda_{P^n}, L)$. Entonces $f(u)$ divide al polinomio ciclotómico

$$\Psi_{P^n}(u) := \prod_{\substack{(A,P)=1 \\ \text{gr } A < \text{gr } P^n}} (u - \lambda_{P^n}^A) = \text{Irr}(u, \lambda_{P^n}, K).$$

Entonces

$$\Psi_{P^n}(u) = \prod_{\sigma_A \in G} (u - \lambda_{P^n}^A), \quad f(u) = \prod_{\sigma_A \in H} (u - \lambda_{P^n}^A)$$

donde para cualquier $A \in R_T$, primo relativo a P , definimos $\sigma_A(\lambda_{P^n}) = \lambda_{P^n}^A$ y donde $G := G_{P^n} = \text{Gal}(K(\Lambda_{P^n})/K)$ y $H := \text{Gal}(k(\Lambda_{P^n})/L)$.

Tenemos $\text{gr } \Psi_{P^n}(u) = \Phi(P^n) = [K(\Lambda_{P^n}) : K] = q^{(n-1)d}(q^d - 1) = |G|$ y $\text{gr } f(u) = [K(\Lambda_{P^n}) : K] = |H|$. Escribimos $\Psi_{P^n}(u) = f(u)g(u)$. Por lo tanto

$$g(u) = \prod_{\sigma_A \in G \setminus H} (u - \lambda_{P^n}^A).$$

Se sigue que $\mathfrak{D}_{K(\Lambda_{P^n})/K} = (\Psi'_{P^n}(\lambda_{P^n})) = \mathfrak{p}_n^\beta$ donde $\beta = nq^{dn} - (n+1)q^{d(n-1)}$ (Proposición 9.6.1) y $\mathfrak{D}_{K(\Lambda_{P^n})/K} = (f'(\lambda_{P^n})) = \mathfrak{p}_n^\delta$. Notemos que

$$\Psi'_{P^n}(u) = f'(u)g(u) + f(u)g'(u) \quad \text{y} \quad \Psi'_{P^n}(\lambda_{P^n}) = f'(\lambda_{P^n})g(\lambda_{P^n}).$$

Puesto que $\mathfrak{D}_{K(\Lambda_{P^n})/K} = \mathfrak{D}_{K(\Lambda_{P^n})/L} \text{con}_{L/K(\Lambda_{P^n})} \mathfrak{D}_{L/K}$ y \mathfrak{p}_L es totalmente ramificado en $K(\Lambda_{P^n})/L$ obtenemos que

$$\begin{aligned} \gamma &= \frac{\beta - \delta}{[K(\Lambda_{P^n}) : L]} = \frac{1}{[K(\Lambda_{P^n}) : L]} (v_{\mathfrak{p}_n}(\Psi'_{P^n}(\lambda_{P^n})) - v_{\mathfrak{p}_n}(f'(\lambda_{P^n}))) \\ &= \frac{1}{[K(\Lambda_{P^n}) : L]} v_{\mathfrak{p}_n} \left(\frac{\Psi'_{P^n}(\lambda_{P^n})}{f'(\lambda_{P^n})} \right) = \frac{1}{[K(\Lambda_{P^n}) : L]} v_{\mathfrak{p}_n}(g(\lambda_{P^n})). \end{aligned}$$

Esto es

$$\gamma = \frac{1}{[K(\Lambda_{P^n}) : L]} v_{\mathfrak{p}_n}(g(\lambda_{P^n})). \quad (9.8)$$

Se tiene $g(\lambda_{P^n}) = \prod_{\sigma_A \in G \setminus H} (\lambda_{P^n} - \lambda_{P^n}^A)$. Definimos la filtración $\mathcal{D}_i := \{\sigma_A \in G \mid v_P(A-1) \geq i\}$, $i = 0, 1, \dots, n-1$. Tenemos $\mathcal{D}_{i+1} \subseteq \mathcal{D}_i$. Si $A \in R_T$ es tal que $v_P(A-1) = t$, entonces $A = 1 + P^t R$ con R y P son primos relativos y

$$\sigma_A(\lambda_{P^i}) = \lambda_{P^i}^A = \lambda_{P^i}^{1+P^t R} = \lambda_{P^i} + (\lambda_{P^i}^{P^t})^R.$$

Por lo tanto $\sigma_A(\lambda_{P^i}) = \lambda_{P^i}$ si y sólo si $t \geq i$, esto es,

$$\mathcal{D}_i = \text{Gal}(K(\Lambda_{P^n})/K(\Lambda_{P^i})).$$

Consideramos $\mathcal{C}_i := \{\sigma_A \in G \setminus H \mid v_P(A-1) = i\} = (G \setminus H) \cap (\mathcal{D}_i \setminus \mathcal{D}_{i+1}) = \mathcal{D}_i \setminus (H \cup \mathcal{D}_{i+1})$.

Por lo tanto

$$\begin{aligned} |\mathcal{C}_i| &= |\mathcal{D}_i| - |\mathcal{D}_i \cap H| - |\mathcal{D}_i \cap \mathcal{D}_{i+1}| + |\mathcal{D}_i \cap \mathcal{D}_{i+1} \cap H| \\ &= |\mathcal{D}_i| - |\mathcal{D}_i \cap H| - |\mathcal{D}_{i+1}| + |\mathcal{D}_{i+1} \cap H|. \end{aligned}$$

Ahora,

$$\begin{aligned} \mathcal{D}_i \cap H &= \text{Gal}(K(\Lambda_{P^n})/LK(\Lambda_{P^i})) \quad \text{y} \\ \mathcal{D}_{i+1} \cap H &= \text{Gal}(K(\Lambda_{P^n})/LK(\Lambda_{P^{i+1}})). \end{aligned}$$

Por lo tanto

$$\begin{aligned} |\mathcal{C}_i| &= [K(\Lambda_{P^n}) : K(\Lambda_{P^i})] - [K(\Lambda_{P^n}) : LK(\Lambda_{P^i})] \\ &\quad - [K(\Lambda_{P^n}) : K(\Lambda_{P^{i+1}})] + [K(\Lambda_{P^n}) : LK(\Lambda_{P^{i+1}})], \quad 0 \leq i \leq n-1. \end{aligned}$$

Por otro lado, tenemos que $\sigma_A \in \mathcal{C}_i$ si y sólo si $A = 1 + P^i R$ con R primo relativo a P . Por tanto, si $\sigma_A \in \mathcal{C}_i$, entonces

$$\lambda_{P^n} - \lambda_{P^n}^A = \lambda_{P^n} - \lambda_{P^n} - (\lambda_{P^n}^{P^i})^R = -\lambda_{P^{n-i}}^R, \quad 0 \leq i \leq n-1.$$

Así $\sigma_A \in \mathcal{C}_i$ si y sólo si $\sigma_A \in G \setminus H$ y $v_{\mathfrak{p}_n}(\lambda_{P^n} - \lambda_{P^n}^A) = v_{\mathfrak{p}_n}(\lambda_{P^{n-i}}^R) = \frac{\Phi(P^n)}{\Phi(P^{n-i})} = q^{id}$.

Tenemos $G \setminus H = \bigcup_{i=0}^{n-1} \mathcal{C}_i$ y $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ para $i \neq j$. Por lo tanto

$$\begin{aligned}
v_{\mathfrak{p}_n}(g(\lambda_{P^n})) &= \sum_{i=0}^{n-1} |\mathcal{C}_i| q^{id} = \sum_{i=0}^{n-1} [K(\Lambda_{P^n}) : K(\Lambda_{P^i})] q^{id} \\
&\quad - \sum_{i=0}^{n-1} [K(\Lambda_{P^n}) : K(\Lambda_{P^{i+1}})] q^{id} \\
&\quad - \sum_{i=0}^{n-1} [K(\Lambda_{P^n}) : LK(\Lambda_{P^i})] q^{id} \\
&\quad + \sum_{i=0}^{n-1} [K(\Lambda_{P^n}) : LK(\Lambda_{P^{i+1}})] q^{id} \\
&= [K(\Lambda_{P^n}) : K] q^0 - [K(\Lambda_{P^n}) : K(\Lambda_{P^n})] q^{(n-1)d} \\
&\quad + \sum_{i=1}^{n-1} [K(\Lambda_{P^n}) : K(\Lambda_{P^i})] q^{(i-1)d} (q^d - 1) \\
&\quad - [K(\Lambda_{P^n}) : K] q^0 + [K(\Lambda_{P^n}) : K(\Lambda_{P^n})] q^{(n-1)d} \\
&\quad - \sum_{i=1}^{n-1} [K(\Lambda_{P^n}) : LK(\Lambda_{P^i})] q^{(i-1)d} (q^d - 1).
\end{aligned}$$

Por tanto

$$\begin{aligned}
v_{\mathfrak{p}_n}(g(\lambda_{P^n})) &= [K(\Lambda_{P^n}) : K] - [K(\Lambda_{P^n}) : K] + \sum_{i=1}^{n-1} [K(\Lambda_{P^n}) : L] \\
&\quad - \sum_{i=1}^{n-1} [K(\Lambda_{P^n}) : LK(\Lambda_{P^i})] [K(\Lambda_{P^i}) : K] \\
&= n[K(\Lambda_{P^n}) : K] - [K(\Lambda_{P^n}) : L] \\
&\quad - \sum_{i=1}^{n-1} [K(\Lambda_{P^n}) : LK(\Lambda_{P^i})] [K(\Lambda_{P^i}) : K].
\end{aligned}$$

Se sigue que

$$\gamma = n \frac{[K(\Lambda_{P^n}) : K]}{[K(\Lambda_{P^n}) : L]} - 1 - \sum_{i=1}^{n-1} t_i,$$

donde

$$\begin{aligned}
 t_i &= \frac{[K(\Lambda_{P^n}) : LK(\Lambda_{P^i})][K(\Lambda_{P^i}) : K]}{[K(\Lambda_{P^n}) : L]} \\
 &= \frac{[K(\Lambda_{P^n}) : K]}{[LK(\Lambda_{P^i}) : K(\Lambda_{P^i})][K(\Lambda_{P^n}) : L]} \\
 &= \frac{[L : K]}{[LK(\Lambda_{P^i}) : K(\Lambda_{P^i})]} = \frac{[L : K]}{[L : L \cap K(\Lambda_{P^i})]} \\
 &= [L \cap K(\Lambda_{P^i}) : K] = [L_i : K].
 \end{aligned}$$

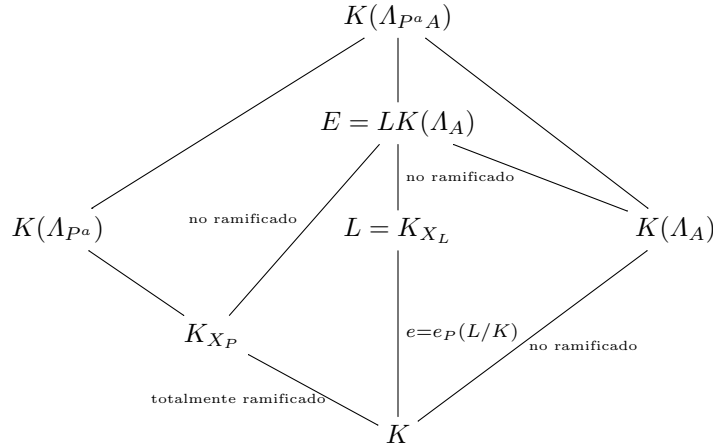
$$\begin{array}{ccc}
 L & \text{-----} & LK(\Lambda_{P^i}) \\
 | & & | \\
 L \cap K(\Lambda_{P^i}) & \text{-----} & K(\Lambda_{P^i})
 \end{array}$$

Por lo tanto

$$\gamma = n[L : K] - \sum_{i=0}^{n-1} [L_i : K]. \quad (9.9)$$

El caso $M = P^n$ se sigue de (9.7) y (9.9).

Para M arbitrario, sea $P \in R_T$ un polinomio mónico e irreducible. Entonces escribimos $M = P^a A$ donde $A \in R_T$ y $P \nmid A$. Sea $E = L(\Lambda_A) = LK(\Lambda_A)$. Se tiene el diagrama (ver Teorema 9.5.4)



Tenemos

$$\mathfrak{D}_{E/K} = \mathfrak{D}_{E/L} \text{ con}_{L/E} \mathfrak{D}_{L/K} = \mathfrak{D}_{E/K_{X_P}} \text{ con}_{K_{X_P}/E} \mathfrak{D}_{K_{X_P}/K}.$$

Denotemos para cualquier extensión E/F y $P \in R_T$, $\mathfrak{d}_{E/F}(P) = P^s$ donde $P^s | \mathfrak{d}_{E/F}$ y $P^{s+1} \nmid \mathfrak{d}_{E/F}$. Entonces

$$\begin{aligned}
 \mathfrak{d}_{E/F}(P) &= (N_{E/K}(\mathfrak{D}_{E/L}))(P) \cdot \mathfrak{d}_{L/K}^{[E:L]}(P) \\
 &= (N_{E/K}(\mathfrak{D}_{E/K_{X_P}}))(P) \cdot \mathfrak{d}_{K_{X_P}/K}^{[E:K_{X_P}]}(P).
 \end{aligned}$$

Puesto que P es no ramificado en E/L y en E/K_{X_P} se tiene

$$(N_{E/L}(\mathfrak{D}_{E/L}))(P) = (N_{E/K}(\mathfrak{D}_{E/K_{X_P}}))(P) = 1.$$

Por tanto

$$\mathfrak{d}_{L/K}(P) = \left(\mathfrak{d}_{K_{X_P}/K}(P) \right)^{[E:K_{X_P}]/[E:L]}.$$

Se tiene $[E : K_{X_P}] = [K(\Lambda_A) : K] = \Phi(A)$ y $[E : L] = [Y : X_L]$ donde Y es el grupo de caracteres de Dirichlet asociado a E . Se tiene $Y = X_P \times \widehat{G_A}$. Se sigue que

$$[E : L] = \frac{|Y|}{|X_L|} = \frac{|X_P| |\widehat{G_A}|}{|X|} = \frac{|X_P| \Phi(A)}{|X|}$$

y

$$\frac{[E : K_{X_P}]}{[E : L]} = \frac{\Phi(A)}{\left(\frac{|X_P| \Phi(A)}{|X|} \right)} = \frac{|X|}{|X_P|} = \frac{[L : K]}{|X_P|} = \frac{edh}{e} = dh$$

donde d es el grado relativo de los divisores primos de L sobre \mathfrak{p} y h el número de estos divisores primos.

Puesto que $K_{X_P} \subseteq K(\Lambda_{P^a})$, de la primera parte de esta demostración obtenemos que $\mathfrak{d}_{K_{X_P}/K}(P) = \prod_{\varphi \in X_P} F_\varphi$. Por lo tanto

$$\mathfrak{d}_{K_X/K}(P) = \left(\prod_{\varphi \in X_P} F_\varphi \right)^{([E:K_{X_P}]/[E:L])} = \left(\prod_{\varphi \in X_P} F_\varphi \right)^{dh} = \prod_{\varphi \in X_P} F_\varphi^{dh}.$$

Del epimorfismo natural $\pi: X_L \rightarrow X_P$, $\chi \mapsto \chi_P$ obtenemos $|\text{núc } \pi| = \frac{|X_L|}{|X_P|} = dh$. Por tanto, para cada $\varphi \in X_P$, $|\pi^{-1}(\varphi)| = dh$. Esto es, para cada $\varphi \in X_P$ hay precisamente dh elementos $\chi \in X$ tales que $\pi(\chi) = \chi_P = \varphi$. Se sigue que

$$\mathfrak{d}_{L/K}(P) = \left(\prod_{\varphi \in X_P} F_\varphi \right)^{dh} = \prod_{\chi \in X} F_{\chi_P}.$$

Finalmente, tenemos que $F_\chi = \prod_P F_{\chi_P}$ para $\chi \in X$ (Teorema 9.4.16) y $\mathfrak{d}_{L/K} = \prod_P \mathfrak{d}_{L/K}(P)$. Por lo tanto

$$\mathfrak{d}_{L/K} = \prod_{\chi \in X_L} F_\chi. \quad \square$$

Extensiones radicales de campos de funciones

10.1. Introducción

El contenido de este capítulo está basado en [62, 63].

Sea L/\mathcal{K} una extensión arbitraria de campos. Decimos que L/\mathcal{K} es una *extensión radical* si existe $\alpha \in L$ tal que $L = \mathcal{K}(\alpha)$ y existe $n \in \mathbb{N}$ tal que $\alpha^n = a \in \mathcal{K}$. En otras palabras α es una raíz del polinomio $x^n - a \in \mathcal{K}[x]$. El elemento α usualmente se representa como $\alpha = \sqrt[n]{a}$.

Más generalmente, una extensión radical L/\mathcal{K} es una extensión generada por raíces de polinomios $x^{n_i} - a_i \in \mathcal{K}[x]$, esto es,

$$L = \mathcal{K}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m}) \quad \text{con} \quad n_i \in \mathbb{N}, \quad a_i \in \mathcal{K}, \quad 1 \leq i \leq m.$$

En la teoría de las extensiones radicales se tienen de manera natural dos grupos que permiten el estudio de tales extensiones.

Definición 10.1.1. Sea L/\mathcal{K} una extensión arbitraria de campos. Se definen

(I) el grupo de torsión de L/\mathcal{K} por

$$T(L/\mathcal{K}) := \{\alpha \in L^* \mid \text{existe } n \in \mathbb{N} \text{ tal que } \alpha^n \in \mathcal{K}\},$$

(II) el grupo de cogalois de L/\mathcal{K} por

$$\text{cog}(L/\mathcal{K}) := \frac{T(L/\mathcal{K})}{\mathcal{K}^*}.$$

Para el estudio de las extensiones radicales, Greither y Harrison [18] desarrollaron una teoría que, en cierta forma, es dual a la teoría de Galois, la cual ha sido generalizada en innumerables direcciones.

Definición 10.1.2 (Ver [18] y [6]). Una extensión finita de campos L/\mathcal{K} se llama

(I) *coseparable* si $L = \mathcal{K}(T(L/\mathcal{K}))$,

- (II) *conormal* si $|\text{cog}(L/\mathcal{K})| \leq [L : \mathcal{K}]$,
 (III) *cogalois* si es conormal y coseparable.

Notemos que coseparable y radical significan lo mismo.

Definición 10.1.3. Una extensión n de Kummer es una extensión L/\mathcal{K} tal que

$$L = \mathcal{K}(\sqrt[n]{\Delta}),$$

donde $n \in \mathbb{N}$ es primo relativo a la característica de \mathcal{K} , $\mu_n \subseteq \mathcal{K}$ donde μ_n es el grupo de las n -ésimas raíces de la unidad y Δ es un subgrupo de \mathcal{K}^* que contiene a \mathcal{K}^{n*} y $\mathcal{K}(\sqrt[n]{\Delta})$ es el campo generado por todas las raíces $\sqrt[n]{a}$ con $a \in \Delta$.

Este es el origen de la *Teoría de Kummer*, la cual es una parte importante en el estudio de los campos de clase. Se tienen los siguientes resultados.

Teorema 10.1.4. Sea \mathcal{K} cualquier campo que contiene al grupo μ_n de las n -raíces de la unidad donde n es primo relativo a la característica de \mathcal{K} . Entonces

- (I) Toda extensión n de Kummer L/\mathcal{K} es una extensión de Galois con grupo de Galois $\text{Gal}(L/\mathcal{K})$ abeliano de exponente n .
 (II) Si L/\mathcal{K} es una extensión abeliana de exponente n , entonces existe un subgrupo $\mathcal{K}^{n*} \subseteq \Delta \subseteq \mathcal{K}^*$ tal que $L = \mathcal{K}(\sqrt[n]{\Delta})$.

Demostración. Ver [50]. □

La analogía existente entre campos numéricos y campos de funciones congruentes, y de manera más precisa, de campos ciclotómicos con campos de funciones ciclotómicos, nos llevan a la pregunta natural si existe lo análogo de la torsión usual con la torsión modular definida por la acción de Carlitz-Hayes.

Daremos una nueva definición de extensión radical usando la acción de Carlitz-Hayes. Así, una extensión L/\mathcal{K} será llamada *radical* si L puede ser generada por algunos elementos u con $u^{M_u} \in \mathcal{K}$ sobre \mathcal{K} , donde M_u son polinomios en R_T . Entre estas extensiones, estamos en especial interesados en las llamadas extensiones *radicales ciclotómicas*. Una extensión se llamará radical ciclotómica si es radical, separable y *pura*. Estas extensiones pueden ser vistas como generalizaciones naturales de las extensiones de Carlitz-Kummer. Estas extensiones tiene propiedades análogas a las extensiones cogalois definidas en [18], ver las Secciones 10.5 y 10.6. Una extensión radical ciclotómica L/\mathcal{K} satisface que $L = \mathcal{K}(T(L/\mathcal{K}))$. Notemos la analogía con la definición previa.

En este capítulo estudiaremos la torsión dada por la acción de Carlitz-Hayes. Por tanto entendemos por “radical” en el sentido de esta acción. Estudiaremos la estructura de campos de funciones congruentes generadas por torsión. En la Sección 10.4 definimos el concepto de extensión radical ciclotómica como un análogo natural de las extensiones cogalois clásicas. Daremos ejemplos tanto de extensiones radicales como de no radicales ciclotómicas así como

de extensiones puras y de extensiones no puras y mostraremos que, como en el caso clásico, la extensión $K(\Lambda_{P^n})/K(\Lambda_P)$ es pura en donde $P \in R_T$ es un polinomio irreducible y $n \in \mathbb{N}$. En las Secciones 10.5 y 10.6 daremos algunas propiedades tanto de extensiones radicales como de extensiones radicales ciclotómicas y probaremos que, como en el caso clásico, para extensiones de Galois, el grupo de cogalois es isomorfo al grupo de los homomorfismos cruzados.

En la Sección 10.7 obtendremos los resultados principales del capítulo: caracterizaremos las extensiones radicales ciclotómicas finitas. En particular, veremos que extensiones radicales finitas son p -extensiones donde p es la característica del campo base. Esto se probará en los Teoremas 10.7.6 y 10.7.7 y en el Corolario 10.7.9. En la Sección 10.8, daremos ejemplos y aplicaciones de estos resultados. Finalmente, en la Sección 10.9 hallaremos una cota superior para la cardinalidad del grupo de cogalois de una extensión radical ciclotómica finita.

Durante este capítulo, usaremos la siguiente notación.

p denota a un número primo.

$q = p^\nu$, $\nu \in \mathbb{N}$.

$K = \mathbb{F}_q(T)$ denota al campo de funciones racionales.

$R_T = \mathbb{F}_q[T]$.

$\mu(\mathcal{K})$ denota al conjunto de las raíces de Carlitz contenidas en un campo \mathcal{K} .

\overline{K} denota a una cerradura algebraica de K .

$\text{car}(L)$ denota a la característica de un campo L .

Si E/L es una extensión de campos tal que $K \subseteq L \subseteq E \subseteq \overline{K}$, denotamos por $T(E/L)$ al conjunto $\{u \in E \mid \text{existe } M \in R_T \text{ tal que } u^M \in L\}$.

C_m denota al grupo cíclico de orden m .

10.2. Extensiones de Kummer de campos de funciones

En esta sección presentaremos una generalización de extensiones de Kummer por medio de la acción de Carlitz–Hayes. En lo que resta en este capítulo p siempre denotará un número primo y $q = p^\nu$ donde $\nu \in \mathbb{N}$. Denotaremos $k = \mathbb{F}_q$, $K = k(T)$ y $R_T = k[T]$. Llamaremos Λ_M , $M \in R_T \setminus \{0\}$, las M -raíces de Carlitz y si λ_M es generador de Λ_M , λ_M se llamará *raíz primitiva de Carlitz*.

Notemos que si $a \in \overline{K}$, entonces el conjunto de todas las raíces del polinomio $z^M - a \in \overline{K}[z]$ es el conjunto $\{\alpha + \lambda \mid \lambda \in \Lambda_M\}$ donde α es cualquier raíz fija $z^M - a$ en \overline{k} .

Necesitaremos varios resultados de teoría de módulos en esta sección.

La Proposición 10.3.2 y el Teorema 10.3.4 son análogos a (I) and (II) del Teorema 10.1.4 con la salvedad que consideraremos únicamente extensiones finitas.

10.2.1. Algo sobre la teoría de módulos

En esta subsección, a menos que se indique lo contrario, todos los módulos y homomorfismos considerados son R_T -módulos y R_T -homomorfismos respectivamente.

Sea A un módulo, $a \in A$. Se define el homomorfismo

$$\varphi_a: R_T \rightarrow A, \quad \text{definido por} \quad \varphi_a(M) := Ma.$$

Definición 10.2.1. Decimos que A es un *módulo cíclico* si existe $a \in A$ tal que φ_a es un epimorfismo.

Notemos que la Definición 10.2.1 es equivalente a decir que existe $a \in A$ tal que $A = (a) = R_T a$.

Para $a \in A$ consideremos el núcleo del homomorfismo φ_a , $\text{núc}(\varphi_a)$. Si $\text{núc}(\varphi_a) \neq \{0\}$ existe un polinomio no cero M , al cual lo podemos suponer sin pérdida de generalidad mónico, tal que $\text{núc}(\varphi_a) = (M)$.

Definición 10.2.2. Sea $a \in A$. Decimos que a tiene *orden infinito* si el núcleo de φ_a es cero. Decimos que a tiene *orden finito* si existe un polinomio mónico $M \in R_T \setminus \{0\}$ tal que $(M) = \text{núc}(\varphi_a) = (M)$. Si A es un módulo, un *exponente* de A es un elemento no cero $M \in R_T$, tal que $Ma = 0$ para todo $a \in A$.

Observación 10.2.3. Si A es un módulo finito, existe $a \in A$ tal que φ_a es un epimorfismo de tal forma que existe $M \in R_T \setminus \{0\}$ tal que

- (I) $\text{núc}(\varphi_a) = (M)$ y
- (II) $R_T/(M) \cong A$.

Como antes, podemos reemplazar a M por un polinomio mónico y entonces diremos que A tiene *orden* M .

La demostración del siguiente lema es directa y no la presentamos.

Lema 10.2.4. Sea A un módulo cíclico de orden N con $N \neq 0$. Sea N_1 un divisor mónico de N . Entonces existe un submódulo de A de orden N_1 . \square

Observación 10.2.5. Con las condiciones del Lema 10.2.4, se sigue de la Observación 10.2.3 que $Na = 0$.

Por otro lado, si B es un submódulo cíclico de A de orden N_1 , entonces nuevamente de la Observación 10.2.3 obtenemos que existe $b \in B$, tal que φ_b es un epimorfismo y $\text{núc}(\varphi_b) = (N_1)$. Puesto que $b \in A$, existe $N_2 \in R_T$, tal que $b = N_2 a$.

Ahora, puesto que $Nb = N(N_2 a) = N_2(Na) = 0$ tenemos que $N \in \text{núc}(\varphi_b) = (N_1)$. Por tanto N_1 es un divisor de N . Puesto que todos los módulos cíclicos de orden M son isomorfos a $R_T/(M)$, esto es, esencialmente únicos, se sigue que para cada divisor mónico M de N , existe un único submódulo cíclico de orden M de A .

Sea A un módulo cíclico con exponente M . Denotamos por C_M al módulo $R_T/(M)$ el cual es cíclico de orden M . Esto en analogía a la notación C_m de los grupos cíclicos.

Definición 10.2.6. Se denota por \hat{A} o por $\text{Hom}_{R_T}(A, C_M)$ al grupo de homomorfismos de A en C_M , donde A es de exponente M . Este módulo se llama el *módulo dual* de A .

Supongamos que $f: A \rightarrow B$ es un homomorfismo, y que tanto A como B tienen exponente M . Entonces se tiene un homomorfismo $\hat{f}: \hat{B} \rightarrow \hat{A}$ definido por $\hat{f}(\psi) = \psi \circ f$. Notemos que $\widehat{(\quad)}$ es un funtor contravariante, es decir

$$\widehat{(\quad)}: R_T\text{-módulos de exponente } M \longrightarrow R_T\text{-módulos}$$

es tal que si $f: A \rightarrow B$ y $g: B \rightarrow C$ son homomorfismos, entonces

- (1) $\widehat{g \circ f} = \hat{f} \circ \hat{g}$ y
- (2) $\widehat{1} = 1$.

Lema 10.2.7. Si A es un módulo finito de exponente M , tal que $A = B \times C$, entonces \hat{A} es isomorfo a $\hat{B} \times \hat{C}$.

Demostración. Las proyecciones naturales $\pi_1: B \times C \rightarrow B$ y $\pi_2: B \times C \rightarrow C$, inducen los homomorfismos $\hat{\pi}_1: \hat{B} \rightarrow \widehat{B \times C}$ y $\hat{\pi}_2: \hat{C} \rightarrow \widehat{B \times C}$, por lo que podemos definir $\theta: \hat{B} \times \hat{C} \rightarrow \widehat{B \times C}$ dada por $\theta(\psi_1, \psi_2) = \hat{\pi}_1(\psi_1) + \hat{\pi}_2(\psi_2)$, donde $(\psi_1, \psi_2) \in \hat{B} \times \hat{C}$.

Se tiene que θ es un homomorfismo. Por otra parte si $\psi \in \widehat{B \times C}$ entonces, puesto que ψ es un homomorfismo, $\psi(x, y) = \psi(x, 0) + \psi(0, y)$ para todo $(x, y) \in B \times C$. Ahora se define $\psi_1: B \rightarrow A_M$ por $\psi_1(x) = \psi(x, 0)$ y $\psi_2: C \rightarrow A_M$ dado por $\psi_2(y) = \psi(0, y)$. Entonces ψ_1 y ψ_2 son homomorfismos. De esta forma se induce una función

$$\delta: \widehat{B \times C} \rightarrow \hat{B} \times \hat{C}$$

dada por $\delta(\psi) = (\psi_1, \psi_2)$ el cual es un homomorfismo de módulos y cuya inversa es θ . El resultado se sigue. \square

Proposición 10.2.8. Un módulo finito A es isomorfo a su dual. Esto es

$$A \cong \hat{A} = \text{Hom}_{R_T}(A, C_M),$$

donde A tiene exponente M .

Demostración. Del Teorema 4.7, Capítulo 5 de [28], tenemos que se puede escribir $A \cong \oplus_P A_P$. La suma anterior es sobre todos los polinomios mónicos irreducibles P y A_P denota los elementos de A que tiene orden una potencia de P .

Ahora por el Teorema 4.9, Capítulo 5 de [28] se tiene que A_P se puede escribir como $A_P \cong C_{P^{\alpha_1}} \oplus \cdots \oplus C_{P^{\alpha_k}}$, donde $\alpha_1 \geq \cdots \geq \alpha_k \geq 1$ y cada $C_{P^{\alpha_i}}$ es un módulo cíclico cuyo generador tiene orden P^{α_i} . De esta forma, cada $C_{P^{\alpha_i}}$ tiene orden P^{α_i} . Nótese que cada A_P y cada $C_{P^{\alpha_i}}$ tiene exponente M .

Por la observación anterior y el Lema 10.2.7, podemos suponer que A es cíclico generado por a de orden P^α , con $\alpha \in \mathbb{N}$ y $P \in R_T$ irreducible. Por lo tanto la función φ_a es un epimorfismo y $(P^\alpha) = \text{núc}(\varphi_a)$.

Puesto que M es de exponente de A , se tiene que $P^\alpha | M$. Ahora del Lema 10.2.4, junto con la Observación 10.2.3, se tiene C_M tiene un único submódulo cíclico de orden P^α , que denotamos por C_{P^α} . El homomorfismo $\varphi_a: R_T \rightarrow A$ induce un isomorfismo, que seguiremos denotando por $\varphi_a: R_T/(P^\alpha) \rightarrow A$.

Al inverso del isomorfismo φ_a , lo denotaremos por ψ . Sea $y = \psi(a)$, entonces y es un generador de C_{P^α} . Al componer ψ con la inclusión natural $C_{P^\alpha} \hookrightarrow C_M$, se obtiene un elemento de \hat{A} , que seguiremos denotando por ψ .

Ahora sea $\varphi \in \hat{A}$. Notemos que $\text{im}(\varphi) \subseteq C_M$ es un submódulo cíclico de orden N . Así, existe $w \in \text{im}(\varphi)$, $w = \varphi(a_w)$ con $a_w \in A$, que genera a $\text{im}(\varphi)$ y su orden es N .

Por otra parte se tiene que $P^\alpha \in (N)$. Por lo tanto $P^\alpha = ND$, para algún $D \in R_T$. Por lo que $N = P^\gamma$ para algún $\gamma \leq \alpha$, es decir, w tiene orden P^γ y como a_w genera a $\text{im}(\varphi)$, se tiene que $\text{im}(\varphi) \subseteq C_{P^\alpha}$.

Por otro lado φ está determinado completamente por su acción en a , donde $a \in A$ es un generador de A . Por lo tanto $\varphi(a) = Ny$. Ahora si $\psi_N = N\psi$ entonces $\psi_N(a) = N\psi(a) = Ny = \varphi(a)$, es decir, $\varphi = \psi_N \in (\psi)$.

De esta forma se tiene $\hat{A} = (\psi)$ el cual es de orden $q^{\text{gr}(P^\alpha)}$. Por lo tanto $A \cong \hat{A}$. \square

Definición 10.2.9. Sean A y B módulos. Una *función bilineal* de $A \times B$ en un módulo C es una función $A \times B \rightarrow C$, denotada por $(a, b) \mapsto \langle a, b \rangle$, que tiene la propiedad siguiente: para cada $a \in A$, la función $b \mapsto \langle a, b \rangle$ es un homomorfismo y, para cada $b \in B$, la función $a \mapsto \langle a, b \rangle$ es un homomorfismo. Un elemento $a \in A$ se dice *ortogonal* a $S \subseteq B$ si $\langle a, b \rangle = 0$ para cada $b \in S$.

De modo análogo tenemos la definición de que $b \in B$ sea ortogonal a $S \subseteq A$, esto es, si $\langle a, b \rangle = 0$ para toda $a \in A$. El *núcleo izquierdo* de la función bilineal es el submódulo de A , que denotamos por N_I , ortogonal a B .

El *núcleo derecho* de la función bilineal es el submódulo de B , que denotamos por N_D , ortogonal a A .

Un elemento $b \in B$ da lugar a un elemento de $\text{Hom}_{R_T}(A, C)$, dado por $a \mapsto \langle a, b \rangle$, que denotamos por ψ_b . Entonces ψ_b se anula en N_I , es decir, $\psi_b(a) = 0$ para cada $a \in N_I$. Así, ψ_b induce un homomorfismo $A/N_I \rightarrow C$, dado por $a + N_I \mapsto \psi_b(a)$.

Por otro lado, si $b \equiv b' \pmod{N_D}$ entonces $\psi_b = \psi_{b'}$, esto da lugar, en primer término, a un homomorfismo $\psi: B/N_D \rightarrow \text{Hom}_{R_T}(A/N_I, C)$ dado por $\psi(b + N_D) = \psi_b$, y, en segundo término, a la sucesión exacta de módulos

$$0 \rightarrow B/N_D \rightarrow \text{Hom}_{R_T}(A/N_I, C). \quad (10.1)$$

De modo similar se obtiene

$$0 \rightarrow A/N_I \rightarrow \text{Hom}_{R_T}(B/N_D, C). \quad (10.2)$$

Proposición 10.2.10. *Sea $A \times A' \rightarrow C$ una función bilineal de módulos, con C un módulo cíclico finito de orden M . Sean B y B' los núcleos izquierdos y derecho, respectivamente. Supongamos que A'/B' es finito. Entonces A/B es finito y A'/B' es isomorfo al módulo dual de A/B .*

Demostración. De las sucesiones exactas (10.1) y (10.2), se deduce que las sucesiones siguientes son exactas

$$0 \rightarrow A'/B' \rightarrow \text{Hom}_{R_T}(A/B, C) \quad (10.3)$$

y

$$0 \rightarrow A/B \rightarrow \text{Hom}_{R_T}(A'/B', C). \quad (10.4)$$

De (10.4) deducimos que A/B puede ser visto como un submódulo de $\text{Hom}_{R_T}(A'/B', C)$, de aquí la finitud de A/B . Por otro lado se tienen las desigualdades, que se infieren de las sucesiones (10.3) y (10.4) y de la Proposición 10.2.8:

$$\text{card}(A/B) \leq \text{card}(\widehat{A'/B'}) = \text{card}(A'/B')$$

y

$$\text{card}(A'/B') \leq \text{card}(\widehat{A/B}) = \text{card}(A/B).$$

La segunda igualdad se debe a la Proposición 10.2.8. De esto se deduce la suprayectividad de la sucesión exacta (10.3), y de esto se sigue el resultado. \square

10.3. Teoría de Kummer

En esta sección se dará una generalización de las extensiones de Kummer, un poco diferente a las dadas por Chi y Li en [12] y por Schultheis en [66]. En lo que sigue supondremos que las extensiones a considerar son subextensiones de \overline{K}/K . Siguiendo a [44], sean $M \in R_T$ un polinomio no constante y $\varphi: \mathcal{K} \rightarrow \mathcal{K}$ definido por $\varphi(u) = u^M$, donde $\mathcal{K} = K(\Lambda_M)$. Entonces φ es un R_T -homomorfismo. Por otra parte consideremos un R_T -submódulo B de \mathcal{K} , bajo la acción de Carlitz Hayes, que contenga a $\mathcal{K}^M = \varphi(\mathcal{K})$.

Denotamos por \mathcal{K}_B la composición de todos los campos $\mathcal{K}(\sqrt[M]{a})$ con $a \in B$. Esto último quiere decir que adjuntamos a \mathcal{K} una raíz arbitraria α de la ecuación $z^M - a = 0$, donde $\alpha \in \overline{K}$. Puesto que las M -raíces de Carlitz están en \mathcal{K} , tal campo no depende de la elección de la raíz α , y por lo tanto \mathcal{K}_B es de Galois sobre \mathcal{K} .

Definición 10.3.1. Diremos que una extensión abeliana L/\mathcal{K} , con grupo de Galois G , es una extensión R_T -abeliana si G tiene estructura de R_T -módulo; una extensión R_T -abeliana L/\mathcal{K} se dice que tiene *exponente* $M \in R_T$ si $M \cdot \sigma = 1$ para cada $\sigma \in G$ (ver [12]).

Proposición 10.3.2. (I) Sea B un R_T -módulo de \mathcal{K} que contiene a \mathcal{K}^M y sea \mathcal{K}_B la composición de todos los campos $\mathcal{K}(\sqrt[M]{a})$, para cada $a \in B$. Entonces $\mathcal{K}_B/\mathcal{K}$ es Galois y abeliana.
 (II) Supongamos que $\mathcal{K}_B/\mathcal{K}$ es una extensión R_T -abeliana y de exponente M . Entonces existe una función bilineal:

$$G \times B \rightarrow \Lambda_M \quad \text{dada por} \quad (\sigma, a) \mapsto \langle \sigma, a \rangle$$

donde $\langle \sigma, a \rangle = \sigma(\alpha) - \alpha$ y α satisface $\alpha^M = a$. El núcleo izquierdo es 1 y el núcleo derecho es \mathcal{K}^M .

La extensión $\mathcal{K}_B/\mathcal{K}$ es finita si y sólo si $(B : \mathcal{K}^M)$ es finito. Si esto ocurre, entonces

$$B/\mathcal{K}^M \cong \widehat{G}.$$

En particular se tiene que

$$[\mathcal{K}_B : \mathcal{K}] = (B : \mathcal{K}^M).$$

Demostración. (I) Sea $b \in B$ y sea β una M -raíz de b . El polinomio $z^M - b$ se descompone en factores lineales en \mathcal{K}_B para todo $b \in B$. Entonces $\mathcal{K}_B/\mathcal{K}$ es una extensión de Galois. Sean $G = \text{Gal}(\mathcal{K}_B/\mathcal{K})$, $\sigma \in G$, $b \in B$ y β una raíz del polinomio $z^M - b$. Entonces $\sigma(\beta) = \beta + \lambda^{M_\sigma}$, para algún $M_\sigma \in R_T$, donde λ es un generador de Λ_M , por lo que se tiene un monomorfismo $G \rightarrow \Lambda_M$, $\sigma \mapsto \lambda^{M_\sigma}$ de donde se sigue que G es un grupo abeliano.

(II) Definimos $G \times B \rightarrow \Lambda_M$ por $(\sigma, b) \mapsto \langle \sigma, b \rangle$, donde $\langle \sigma, b \rangle = \sigma(\beta) - \beta$ y $\beta^M = b$. Esta definición es independiente de la elección de la M -raíz de b . Se tiene que $\langle \sigma, a + b \rangle = \langle \sigma, a \rangle + \langle \sigma, b \rangle$ para cada $a, b \in B$ y puesto que $(\sigma(\beta) - \beta) \in \Lambda_M$, se sigue que $\langle \sigma \cdot \tau, b \rangle = \langle \sigma, b \rangle + \langle \tau, b \rangle$.

Sea $\sigma \in G$ y supongamos que $\langle \sigma, b \rangle = 0$ para cada $b \in B$. Por lo tanto, si β satisface que $\beta^M = b$ se tiene que $\sigma(\beta) = \beta$, y como esto vale para cada generador se tiene que $\sigma = 1$, es decir el núcleo izquierdo es 1.

Por otro lado si $b \in B$ satisface que $\langle \sigma, b \rangle = 0$ para todo $\sigma \in G$ entonces $\sigma(\beta) = \beta$ para toda $\sigma \in G$. Por lo tanto, $\beta \in \mathcal{K}$ y $b = \beta^M \in \mathcal{K}^M$. De aquí se sigue que el núcleo derecho es \mathcal{K}^M .

Ahora supongamos que B/\mathcal{K}^M es finito. Entonces $G/1 = G$ es finito. En particular $\mathcal{K}_B/\mathcal{K}$ es finito. Ahora bien, si $\mathcal{K}_B/\mathcal{K}$ es finito, puesto que el núcleo derecho es \mathcal{K}^M , de la Proposición 10.2.10 se obtiene que la siguiente sucesión es exacta

$$0 \rightarrow B/\mathcal{K}^M \rightarrow \text{Hom}_{R_T}(G/1, \Lambda_M).$$

De esta sucesión y de que $\text{Hom}_{R_T}(G/1, \Lambda_M)$ es finito, se sigue que $(B : \mathcal{K}^M)$ es finito.

Finalmente, puesto que por la Proposición 10.2.8 B/\mathcal{K}^M es isomorfo al módulo dual de G , se tiene que $B/\mathcal{K}^M \cong G$, así que $[\mathcal{K}_B : \mathcal{K}] = (B : \mathcal{K}^M)$. \square

Antes de mostrar la proposición siguiente necesitamos algunas definiciones, dadas en [12].

Definición 10.3.3. Una extensión R_T -abeliana L/\mathcal{K} se dice que es R_T -cíclica si $\text{Gal}(L/\mathcal{K})$ es un R_T -módulo cíclico. En este caso si $\text{Gal}(L/\mathcal{K}) \cong R_T/(M)$, con M un polinomio mónico, diremos que L/\mathcal{K} es una extensión cíclica de orden M .

En el siguiente teorema denotamos por \mathfrak{M} el conjunto de R_T -submódulos de \mathcal{K} , que contienen a \mathcal{K}^M y \mathfrak{F} denota el conjunto de extensiones R_T -abelianas de \mathcal{K} de exponente M .

Teorema 10.3.4. Con las notaciones de la Proposición 10.3.2, la función $\varphi : \mathfrak{M} \rightarrow \mathfrak{F}$ dada por $\varphi(B) = \mathcal{K}_B$ es inyectiva. Además si L/\mathcal{K} es una extensión R_T -abeliana, finita, de exponente M entonces existe un R_T -submódulo B , de \mathcal{K} , que contiene a \mathcal{K}^M , tal que $L = \mathcal{K}_B$.

Demostración. Para mostrar la inyectividad de la función anterior bastará probar que si $\mathcal{K}_{B_1} \subseteq \mathcal{K}_{B_2}$ entonces $B_1 \subseteq B_2$, puesto que de la igualdad $\varphi(B_1) = \varphi(B_2)$, se deducen las contenciones $\mathcal{K}_{B_1} \subseteq \mathcal{K}_{B_2}$ y $\mathcal{K}_{B_2} \subseteq \mathcal{K}_{B_1}$.

Sea $b \in B_1$. Se tiene que $\mathcal{K}(\sqrt[M]{b}) \subseteq \mathcal{K}_{B_2}$ por lo que $\mathcal{K}(\sqrt[M]{b})$ está contenido en una subextensión finitamente generada de \mathcal{K}_{B_2} , es decir, existen un número finito de elementos $b_i \in B_2$ de modo que $\mathcal{K}(\sqrt[M]{b}) \subseteq \mathcal{K}(b_1, \dots, b_m)$. Así podemos suponer que B_2/\mathcal{K}^M es finitamente generada y por tanto es una extensión finita.

Sea β tal que $\beta^M = b$. Sea B_3 el submódulo de \mathcal{K} generado por B_2 y b . Veamos $\mathcal{K}_{B_2} = \mathcal{K}_{B_3}$. Tenemos que $\mathcal{K}_{B_2} \subseteq \mathcal{K}_{B_3}$. Para mostrar la otra contención, sea α una raíz M -ésima de $c \in B_3$. Si $c \in B_2$ entonces $\mathcal{K}(\alpha) \subseteq \mathcal{K}_{B_2}$. Si c es de la forma $b^N + \sum b_i^{N_i}$, con $b_i \in B_2$, entonces $\alpha^M = b^N + \sum b_i^{N_i} = \beta^{MN} + \sum \beta_i^{MN_i}$, con $\beta_i^M = b_i$, $i = 1, \dots, s$, es decir, $\alpha = \beta^N + \sum \beta_i^{N_i} + \lambda^A$, donde λ es un generador de Λ_M . Por lo tanto $\mathcal{K}(\alpha) \subseteq \mathcal{K}_{B_2}$. De aquí se sigue que $\mathcal{K}_{B_3} \subseteq \mathcal{K}_{B_2}$.

Entonces, por la Proposición 10.3.2 (II) se tiene $(B_2 : \mathcal{K}^M) = (B_3 : \mathcal{K}^M)$, de esta manera $b \in B_2$, por lo que $B_1 \subseteq B_2$.

Por otro lado, sea \mathcal{K}' una extensión R_T -abeliana de \mathcal{K} de exponente M , finita. Sea $G = \text{Gal}(\mathcal{K}'/\mathcal{K})$. Entonces, por los Teoremas 4.7 y 4.9, Capítulo 4 de [28], G es suma directa, finita, de R_T -submódulos de exponente M . Aplicando Teoría de Galois podemos suponer que la extensión es cíclica de exponente M . Ahora por la Proposición 2.6 de [12], se tiene que toda extensión cíclica \mathcal{K}'/\mathcal{K} de exponente M , se obtiene adjuntando una M -raíz de un elemento de \mathcal{K} .

Así \mathcal{K}' es la adjunción de M -raíces, es decir, existen $\{b_j\} \subseteq \mathcal{K}$ y $\{\alpha_j\} \subseteq \mathcal{K}'$ tales que $\alpha_j^M = b_j$ y $\mathcal{K}' = \mathcal{K}(\{\alpha_j\})$. Sea B el submódulo de \mathcal{K} generado

por $\{b_j\}$ y \mathcal{K}^M . Entonces $\mathcal{K}' \subseteq \mathcal{K}_B$. Por otro lado consideremos una raíz M -ésima de $c \in B$, digamos α . Así $\alpha^M = c$. Se tiene que $c = \sum_{j=1}^s b_j^{N_j} + a^M$, $a \in \mathcal{K}$. Entonces $\alpha = \sum_{j=1}^s \alpha_j^{N_j} + a$ por lo que $\mathcal{K}(\alpha) \subseteq \mathcal{K}'$. Se sigue que $\mathcal{K}_B \subseteq \mathcal{K}'$ y $\varphi(B) = \mathcal{K}'$. Esto termina la demostración. \square

Proposición 10.3.5. *Sea L/\mathcal{K} una extensión R_T -abeliana, finita, supongamos que $\Lambda_N \subseteq \mathcal{K}$, con $N \in R_T$ no constante. Sea*

$$W = \{\bar{\alpha} = \alpha + \mathcal{K}^N \in \mathcal{K}/\mathcal{K}^N \mid \sqrt[N]{\alpha} \in L\}.$$

Entonces $W \cong \text{Hom}(G, \Lambda_N)$, donde $G = \text{Gal}(L/\mathcal{K})$.

Demostración. Dado $\bar{\alpha} \in W$, se define una función $\varphi_{\bar{\alpha}} : G \rightarrow \Lambda_N$ definida así $\varphi_{\bar{\alpha}}(\sigma) = \sigma(\alpha) - \alpha$, donde α es una raíz N -ésima de a ; $\varphi_{\bar{\alpha}}$ es independiente de la raíz usada. Notemos que

$$\begin{aligned} \varphi_{\bar{\alpha}}(\sigma \circ \tau) &= \sigma(\tau(\alpha)) - \alpha = \sigma(\tau(\alpha) - \alpha + \alpha) - \alpha \\ &= \sigma(\tau(\alpha) - \alpha) + \sigma(\alpha) - \alpha = \tau(\alpha) - \alpha + \sigma(\alpha) - \alpha. \end{aligned}$$

Por tanto $\varphi_{\bar{\alpha}}$ es un homomorfismo de grupos abelianos. Por lo tanto es posible definir $f : W \rightarrow \text{Hom}(G, \Lambda_N)$ dado por $f(\bar{\alpha}) = \varphi_{\bar{\alpha}}$.

Se tiene que f es un homomorfismo de grupos abelianos. Ahora si $f(\bar{a}) = \varphi_{\bar{a}} = 0$ entonces $\sigma(\alpha) - \alpha = 0$, para cada $\sigma \in G$. De esta manera se tiene que $\alpha \in \mathcal{K}$. Puesto que $a = \alpha^N$, entonces $a \in \mathcal{K}$. De esta modo $\bar{a} = 0$, por lo tanto f es inyectiva.

Ahora sea $\varphi : G \rightarrow \Lambda_N$ un homomorfismo de grupos abelianos. Entonces

$$\varphi(\sigma \circ \tau) = \varphi(\sigma) + \varphi(\tau) = \varphi(\sigma) + \sigma(\varphi(\tau)),$$

es decir, φ es un homomorfismo cruzado, por lo tanto por el Teorema 90 de Hilbert aditivo, existe un $\alpha \in L$ tal que $\varphi(\sigma) = \sigma(\alpha) - \alpha$. Así tenemos $(\sigma(\alpha) - \alpha)^N = \sigma(\alpha^N) - \alpha^N = 0$, por lo que $a = \alpha^N \in \mathcal{K}$, lo cual prueba la suprayectividad de f . \square

10.4. Extensiones radicales ciclotómicas.

Los siguientes resultados serán útiles en esta sección.

Proposición 10.4.1. *Sean $q > 2$, $M \in R_T$ no constante. Consideremos la extensión $K(\Lambda_M)/K$. Entonces $\mu(K(\Lambda_M)) = \Lambda_M$.*

Demostración. Sea $\mu(\Lambda_M) = \Lambda_N$. Puesto que $\Lambda_M \subseteq \mu(\Lambda_M)$, si para un polinomio irreducible $P \in R_T$ y $\alpha \in \mathbb{Z}$, $\alpha \geq 0$, tenemos que $P^\alpha \mid M$, entonces $P^\alpha \mid N$. Si $P^{\alpha+1} \nmid M$, no podemos tener que $P^{\alpha+1} \mid N$ puesto que en caso contrario el índice de ramificación de P en $K(\Lambda_M)/K$ debe ser dividido por

$\Phi(P^{\alpha+1}) = [K(\Lambda_{P^{\alpha+1}}) : K]$, pero la ramificación de P en $K(\Lambda_M)/K$ es $\Phi(P^\alpha)$. Así $N = M$. \square

En lo que sigue, a menos que se especifique otra cosa, las extensiones de campos consideradas L/\mathcal{K} satisfacen que $K \subseteq \mathcal{K} \subseteq L \subseteq \bar{K}$. Por otro lado a las extensiones anteriores se les da estructura de R_T -módulo, usando la acción de Carlitz Hayes definida anteriormente. El primer objeto a considerar, asociado a la extensión L/\mathcal{K} , es el siguiente:

$$T(L/\mathcal{K}) = \{u \in L \mid \text{existe un } M \in R_T \setminus \{0\} \text{ tal que } u^M \in \mathcal{K}\}.$$

Nótese que $T(L/\mathcal{K}) \subseteq L$ es un subgrupo del grupo *aditivo* L . Por otro lado $T(L/\mathcal{K})$ es un R_T -módulo y el R_T -módulo $T(L/\mathcal{K})/\mathcal{K}$ es de R_T -torsión. A este último R_T -módulo lo denotamos por $\text{cog}(L/\mathcal{K})$. Se tiene que $\text{cog}(L/\mathcal{K})$ es análogo al grupo $T(L/\mathcal{K})/\mathcal{K}^*$, en el caso de una extensión L/\mathcal{K} de campos y $T(L/\mathcal{K})$ denota el grupo de torsión usual, ver [6] p.2.

Definición 10.4.2. Diremos que una extensión L/\mathcal{K} es *radical* si existe un subconjunto $A \subseteq T(L/\mathcal{K})$ tal que $L = \mathcal{K}(A)$. Decimos que L/\mathcal{K} es *pura* si para cada polinomio mónico irreducible $M \in R_T$ y cada $u \in L$ tal que $u^M = 0$ se tiene que $u \in \mathcal{K}$. Finalmente diremos que L/\mathcal{K} es una extensión *radical ciclotómica* si:

- (1) es radical,
- (2) separable y
- (3) pura.

Al módulo $\text{cog}(L/\mathcal{K}) = T(L/\mathcal{K})/\mathcal{K}$ lo llamaremos *módulo de cogalois de la extensión*.

A continuación probamos un resultado debido a Schultheis [66].

Teorema 10.4.3. Sean \mathcal{K} una extensión finita de $K(\Lambda_M)$ y $z \in \mathcal{K} \setminus \mathcal{K}^M$ y $F(u) = u^M - z$. Sean $F_1(u), \dots, F_s(u)$ los distintos factores irreducibles de $F(u)$ en $\mathcal{K}[u]$ y sea $\alpha \in \bar{K}$ cualquier raíz de $F_1(u)$. Entonces el campo de descomposición de $F(u)$ sobre \mathcal{K} es $\mathcal{K}(\alpha)$. Además la extensión $\mathcal{K}(\alpha)/\mathcal{K}$ es elemental abeliana y en particular $[\mathcal{K}(\alpha) : \mathcal{K}] = p^t$ para algún $t \in \mathbb{N} \cup \{0\}$.

Demostración. Puesto que las raíces de $F(u)$ son los elementos del conjunto $\{\alpha + \lambda \mid \lambda \in \Lambda_M\}$, se sigue que $\mathcal{K}(\alpha)$ es el campo de descomposición de $F(u)$. Si $G := \text{Gal}(\mathcal{K}(\alpha)/\mathcal{K})$, definimos $\varphi: G \rightarrow \Lambda_M$ por $\varphi(\sigma) = \lambda_\sigma \in \Lambda_M$ donde $\sigma(\alpha) = \alpha + \lambda_\sigma$. Claramente φ es un monomorfismo de grupos y puesto que Λ_M es un p -grupo elemental abeliano, se sigue G lo es y en particular $|G| = [\mathcal{K}(\alpha) : \mathcal{K}] = p^t$ para algún $t \in \mathbb{N} \cup \{0\}$. \square

Ejemplo 10.4.4. La extensión $K(\Lambda_M)/K$, con $M \in R_T$, es radical ya que existe $W = \Lambda_M \subseteq T(K(\Lambda_M)/K)$ tal que $K(\Lambda_M) = K(W)$, es separable, pero no pura, ya que por la Proposición 10.4.1, se tiene que la únicas raíces de Carlitz que estan en $K(\Lambda_M)$ son Λ_M y si Q es un factor irreducible de M , $\lambda_Q \in \Lambda_M$, pero no está en K . Por lo tanto $K(\Lambda_M)/K$ no es una extensión radical ciclotómica. \square

El siguiente ejemplo muestra la existencia de extensiones radicales ciclotómicas.

Ejemplo 10.4.5. Sea p un primo impar, $q = p$ y $M = T$. Considere la extensión $K(\Lambda_M)/K$ cuyo grado es $q - 1 = p - 1$. Se ha visto que $K(\Lambda_M)/K$ no es pura, ver Ejemplo 10.4.4. Ahora considere el polinomio $F(X) = X^T - 1 = X^p + XT - 1$.

Se afirma que $1 \in K(\Lambda_M) \setminus K(\Lambda_M)^M$, ya que si ocurre lo contrario, existe un $u \in K(\Lambda_M)$ tal que $u^M = 1$. Sea α un generador de Λ_M . Notemos que $[K(\alpha) : K] = p - 1$, por lo que $\{1, \alpha, \alpha^2, \dots, \alpha^{p-2}\}$ es una base de $K(\Lambda_M)$ sobre K .

Por lo tanto u se puede escribir como $u = a_0 + a_1\alpha + \dots + a_{p-2}\alpha^{p-2}$ con $a_0, a_1, \dots, a_{p-2} \in K$. Por lo tanto

$$\begin{aligned} u^T &= a_0^T + (a_1\alpha)^T + \dots + (a_{p-2}\alpha^{p-2})^T \\ &= (a_0^p + a_0T) + (a_1^p\alpha^p + a_1\alpha T) + \dots + (a_{p-2}^p\alpha^{p(p-2)} + a_{p-2}\alpha^{p-2}T) \end{aligned} \quad (10.5)$$

Como $\alpha^T = \alpha^p + \alpha T = 0$ entonces $\alpha^p = -\alpha T$. Por lo tanto, puesto que $u^T = 1$, de (10.5) se obtiene

$$\begin{aligned} 1 &= (a_0^p + a_0T) + (a_1^p\alpha^p + a_1\alpha T) + \dots + (a_{p-2}^p\alpha^{p(p-2)} + a_{p-2}\alpha^{p-2}T) \\ &= (a_0^p + a_0T) + (-a_1^p\alpha T + a_1\alpha T) + \dots + (-a_{p-2}^p\alpha^{p-2}T^{p-2} + a_{p-2}\alpha^{p-2}T) \end{aligned}$$

es decir

$$0 = (a_0^p + a_0T - 1) + c_1\alpha + c_2\alpha^2 + \dots + c_{p-2}\alpha^{p-2}$$

donde $c_i = (-1)^i a_i^p T^i + a_i T$, $i = 1, \dots, p - 2$, pertenecen a K .

Por lo tanto llegamos a la ecuación

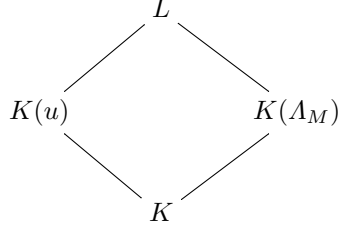
$$0 = a_0^p + a_0T - 1 \quad (10.6)$$

ya que $\{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ es base de $K(\Lambda_M)$ sobre K . En particular $a_0 \neq 0$. Sea $a_0 = \frac{f(T)}{g(T)}$, con $(f(T), g(T)) = 1$, de aquí derivamos la ecuación $f^p(T) + f(T)g^{p-1}(T)T = g^p(T)$. Se sigue que $f(T), g(T) \in \mathbb{F}_q^*$ y por lo tanto $a_0 \in \mathbb{F}_q^*$ lo cual contradice (10.6).

Sea L el campo de descomposición de $F(X)$, sobre $K(\Lambda_M)$, entonces la extensión $L/K(\Lambda_M)$ es separable. Del Teorema 10.4.3 obtenemos que $[L : K(\Lambda_M)] = p^t$, con $t \geq 1$. Si β es una raíz de $F(X)$ se tiene que $L = K(\Lambda_M)(\beta)$, así la extensión $L/K(\Lambda_M)$ es radical. Notemos que como el polinomio irreducible de β divide a $F(X) = X^p + XT - 1$, entonces tal irreducible es $F(X)$. En particular de esto se deduce que $t = 1$.

Para mostrar que la extensión $L/K(\Lambda_M)$ es radical ciclotómica, bastará mostrar que es pura, puesto que hemos mostrado que es radical y separable. Para este fin considere polinomios mónicos irreducibles N , con grado de $N > 1$ y sea $u \in L$ tal que $u^N = 0$. Se afirma que $u = 0$ pues en caso

contrario $u \neq 0$ es un generador de Λ_N , debido a que N es irreducible y a la Proposición 12.2.21 de [70] Capítulo 12. Así se puede considerar el diagrama



Ahora del Teorema 9.2.25 se tiene $[K(u) : K] = \Phi(N) = p^{\text{gr}(N)} - 1 \geq p(p-1) = [L : K]$, pero esto contradice que $[K(u) : K] \mid [L : K]$. Por lo tanto $u = 0 \in K(\Lambda_M)$. Esto muestra la propiedad (3) de la Definición 10.4.2, para los polinomios de grado mayor que 1.

Resta mostrar la propiedad (3) de la Definición 10.4.2, para los polinomios de grado 1. Para ello se consideran los polinomios $T, T+1, \dots, T+(p-1)$. Bastará considerar, por ejemplo, $N = T+1$. Sea $u \in L$ tal que $u^{T+1} = 0$ y supongamos que $u \notin K(\Lambda_M)$, en particular $u \neq 0$. De esta manera $\text{Irr}(u, X, K(\Lambda_M)) \mid (X^{p-1} + T + 1)$, pero esto contradice nuestra suposición de que $\text{gr}(\text{Irr}(u, X, K(\Lambda_M))) = p$. Por lo tanto $u \in K(\Lambda_M)$. \square

Para el siguiente ejemplo necesitamos la siguiente proposición

Proposición 10.4.6. *Sea $q > 2$, $P \in R_T$ mónico e irreducible y $n \in \mathbb{N}$. Entonces la extensión $K(\Lambda_{P^n})/K(\Lambda_P)$ es pura.*

Demostración. Si $\lambda_Q \in K(\lambda_{P^n})$, entonces Q es ramificado en $K(\lambda_{P^n})/K$ lo cual implica que $Q = P$, por la Proposición 12.3.14. Capítulo 12 de [70]. Por lo tanto $K(\lambda_{P^n})/K(\lambda_P)$ es pura. \square

Ejemplo 10.4.7. La extensión $K(\Lambda_{P^n})/K(\Lambda_P)$ es radical ciclotómica, ya que, ciertamente, es radical, separable ya que el polinomio, con coeficientes en R_T , U^{P^n} , es separable y por la Proposición 10.4.6 la extensión es pura. \square

10.5. Algunas propiedades de las extensiones radicales.

Las extensiones radicales L/\mathcal{K} estudiadas aquí, tienen propiedades análogas a las extensiones radicales usuales consideradas en [18] y en [2].

Definición 10.5.1. Si G es un módulo de torsión se pondrá

$$\mathcal{O}_G = \{\text{ord}(g) \mid g \in G\}.$$

Definición 10.5.2. Un módulo G se dice *acotado* si G es un módulo de torsión y los grados de los elementos de $\mathcal{O}_G \subseteq R_T$ forman un conjunto acotado, o de modo equivalente, \mathcal{O}_G es finito.

Sea A un R_T -módulo de torsión. Consideremos \mathcal{O}_A . Supongamos que A es un R_T -módulo acotado. Al mínimo común múltiplo de los elementos de \mathcal{O}_A , lo llamaremos el R_T -exponente de A o, si el contexto lo permite, el exponente de A , y lo denotamos por $\text{ex}(A)$.

Ahora sea E/F una extensión radical, no necesariamente finita. Existe un subconjunto $A \subseteq T(E/F)$ tal que $E = F(A)$. Podemos reemplazar A por el submódulo de E generado por A y F , que seguiremos denotando por A .

Ahora A/F es un R_T -módulo de torsión, por lo que tiene sentido considerar $\mathcal{O}_{A/F}$. Diremos que una extensión de R_T -torsión, E/F , es una *extensión acotada* si A/F es un R_T -módulo acotado, en este caso si $N = \text{ex}(A/F)$, diremos que E/F es una extensión N *acotada*.

En este contexto se tiene la siguiente proposición.

Proposición 10.5.3. *Sea E/F una extensión radical acotada, no necesariamente finita, y sea $N = \text{ex}(A/F)$. Entonces E/F es de Galois si y sólo si $\lambda_M \in E$ para todo $M \in \mathcal{O}_{A/F}$.*

Demostración. Sea $\alpha \in E$ cuyo orden es $M \in R_T$. Así tenemos que $\alpha^M = a \in F$. Consideremos el polinomio $f(X) = X^M - a = \prod_N (X - (\alpha + \lambda_M^N)) \in F[X]$. Por lo tanto los conjugados de α son

$$\{\alpha + \xi_1, \dots, \alpha + \xi_s\}$$

para algunos $\xi_i \in A_M$.

Supongamos que la extensión E/F es Galois. Sea B el R_T -módulo generado por $\{\xi_1, \dots, \xi_s\}$. Entonces $B \subseteq E$ y existe un $M' \in R_T$, que divide a M , tal que $B = A_{M'}$. Si $M' \neq M$, entonces $\alpha^{M'} = a' \in F$ lo cual es una contradicción. Por lo tanto $M' = M$ y $\lambda_M \in E$.

Ahora supongamos que $\lambda_M \in E$ para todo $M \in \mathcal{O}_{A/F}$. Sea $u \in A$ y $M = \text{ord}(u)$. Puesto que todo conjugado de u , sobre F , es de la forma $u + \lambda_M^N \in E$, se sigue que la extensión E/F es normal, y como u es separable sobre F , entonces E/F es una extensión de Galois. \square

En algunas extensiones radicales L/\mathcal{K} , es posible encontrar un elemento primitivo explícito y que pertenezca $\text{cog}(L/\mathcal{K})$, como lo muestra la siguiente proposición.

Proposición 10.5.4. *Sea L/\mathcal{K} es una extensión tal que $L = \mathcal{K}(\alpha, \beta)$ y existen $M, N \in R_T$ con $\alpha^M = a$, $\beta^N = b$, $a, b \in \mathcal{K}$, M y N primos relativos. Entonces $L = \mathcal{K}(\alpha + \beta)$, es decir, $\alpha + \beta$ es un elemento primitivo.*

Demostración. Puesto que $\alpha + \beta \in \mathcal{K}(\alpha, \beta)$ se tiene $\mathcal{K}(\alpha + \beta) \subseteq \mathcal{K}(\alpha, \beta)$. Por otro lado $(\alpha + \beta)^M = \alpha^M + \beta^M = a + \beta^M \in \mathcal{K}(\alpha + \beta)$ y $(\alpha + \beta)^N = \alpha^N + \beta^N = \alpha^N + b \in \mathcal{K}(\alpha + \beta)$. Por lo tanto se tiene que $\beta^M, \alpha^N \in \mathcal{K}(\alpha + \beta)$.

Ahora puesto que existen $S_1, S_2 \in R_T$ tales que $1 = MS_1 + NS_2$ se tiene que

$$\alpha = \alpha^1 = \alpha^{MS_1 + NS_2} = a^{S_1} + (\alpha^N)^{S_2} \in \mathcal{K}(\alpha + \beta)$$

y

$$\beta = \beta^1 = \beta^{MS_1 + NS_2} = (\beta^N)^{S_1} + b^{S_2} \in \mathcal{K}(\alpha + \beta).$$

Así pues, $\mathcal{K}(\alpha, \beta) = \mathcal{K}(\alpha + \beta)$. Más aún, $(\alpha + \beta)^{MN} = (\alpha^M)^N + (\beta^N)^M \in \mathcal{K}$. \square

En particular, con las hipótesis de la Proposición 10.5.4, se tiene que

$$[L : \mathcal{K}] \leq |\text{cog}(L/\mathcal{K})|.$$

Notemos que el argumento de la Proposición 10.5.4 se puede generalizar a extensiones de la forma L/\mathcal{K} , con $L = \mathcal{K}(\alpha_1, \dots, \alpha_s)$ de modo que existen $M_i \in R_T$ con $\alpha_i^{M_i} = a_i \in \mathcal{K}$ y los polinomios M_i primos relativos a pares.

10.6. Algunas propiedades de las extensiones radicales ciclotómicas

Las extensiones radicales ciclotómicas tiene algunas propiedades análogas a las propiedades de las extensiones cogalois clásicas. Necesitamos primero un lema.

Lema 10.6.1. *Sea $\mathcal{K} \subseteq L \subseteq L'$ una torre de campos. Entonces L'/\mathcal{K} es pura si y sólo si L'/L y L/\mathcal{K} son puras.*

Demostración. Supongamos que L'/\mathcal{K} es pura. Sean $\lambda \in L'$ y $P \in R_T$, mónico e irreducible, tal que $\lambda_P^P = 0$. Entonces $\lambda_P \in \mathcal{K} \subseteq L$, puesto que L'/\mathcal{K} es pura. Por lo tanto L'/L es pura. De modo completamente análogo se prueba que L/\mathcal{K} es pura.

Por otro lado supongamos que L'/L y L/\mathcal{K} son puras. Sean $\lambda_P \in L'$ y $P \in R_T$, mónico e irreducible, tal que $\lambda_P^P = 0$. Puesto que L'/L es pura, $\lambda_P \in L$ y como L/\mathcal{K} es pura, entonces $\lambda_P \in \mathcal{K}$. \square

Proposición 10.6.2. *Sea $\mathcal{K} \subseteq L \subseteq L'$ una torre de campos. Se tienen las siguientes propiedades.*

(1) *Existe una sucesión exacta de R_T -módulos*

$$0 \rightarrow \text{cog}(L/\mathcal{K}) \rightarrow \text{cog}(L'/\mathcal{K}) \rightarrow \text{cog}(L'/L).$$

(2) *Si la extensión L'/\mathcal{K} es radical ciclotómica, entonces la extensión L'/L es radical ciclotómica.*

- (3) Si la extensión L'/\mathcal{K} es radical, y las extensiones L'/L y L/\mathcal{K} son radicales ciclotómicas, entonces L'/\mathcal{K} es radical ciclotómica.

Demostración. (1) El homomorfismo canónico

$$\text{cog}(L'/\mathcal{K}) \rightarrow \text{cog}(L'/L), \quad x + \mathcal{K} \mapsto x + L$$

es un R_T -homomorfismo con núcleo $\text{cog}(L/\mathcal{K})$. Esto prueba que la sucesión de R_T -módulos

$$0 \rightarrow \text{cog}(L/\mathcal{K}) \rightarrow \text{cog}(L'/\mathcal{K}) \rightarrow \text{cog}(L'/L)$$

es exacta.

(2) Como L'/\mathcal{K} es separable, entonces L'/\mathcal{K} es separable y, por el Lema 10.6.1, L'/\mathcal{K} es pura. Finalmente puesto que $T(L'/\mathcal{K}) \subseteq T(L'/L)$ se tiene que L'/L es radical.

(3) Como L'/L y L/\mathcal{K} son extensiones radicales ciclotómicas entonces ambas son separables y puras. Por lo tanto, por el Lema 10.6.1, la extensión L'/\mathcal{K} es pura, además separable. Se sigue que L'/\mathcal{K} es una extensión radical ciclotómica. \square

Veremos que para algunas extensiones L/\mathcal{K} se tiene que el R_T -módulo $\text{cog}(L/\mathcal{K})$ es finito. Para empezar considere L/\mathcal{K} una extensión de Galois de campos de funciones, con grupo de Galois $G = \text{Gal}(L/\mathcal{K})$. Notemos que $\mu(L)$ es un G -módulo, mediante la acción siguiente: dado $\sigma \in G$ y $u \in \mu(L)$ pongamos $\sigma \cdot u = \sigma(u)$. Puesto que la acción de Carlitz Hayes conmuta con σ , $\sigma \cdot u$ está bien definida.

Definición 10.6.3. Una función $f : G \rightarrow \mu(L)$ se dice que es un *homomorfismo cruzado de G con coeficientes en $\mu(L)$* si para cada $\sigma, \tau \in G$ se tiene que $f(\sigma \circ \tau) = f(\sigma) + \sigma \cdot f(\tau)$.

Al conjunto de homomorfismos cruzados los denotamos por

$$Z^1(G, \mu(L)),$$

y $B^1(G, \mu(L))$ denota al subconjunto de $Z^1(G, \mu(L))$ dado por

$$\{\chi \in Z^1(G, \mu(L)) \mid \text{existe } u \in \mu(L) \text{ tal que } \chi = f_u\},$$

donde f_u es la función definida por

$$f_u(\sigma) := \sigma u - u \quad \text{para cada } \sigma \in G.$$

Teorema 10.6.4. Sea L/\mathcal{K} una extensión finita de Galois, G su grupo de Galois. Entonces la función $\phi : \text{cog}(L/\mathcal{K}) \rightarrow Z^1(G, \mu(L))$, dada por $\phi(u + \mathcal{K}) = f_u$ donde $f_u(\sigma) = \sigma(u) - u$, es un isomorfismo de grupos.

Demostración. Se define $\theta : T(L/\mathcal{K}) \rightarrow Z^1(G, \mu(L))$ mediante $\theta(u) = f_u$. Obsérvese que $f_u(\sigma \circ \tau) = \sigma(\tau(u)) - u$, además $f_u(\sigma) = \sigma(u) - u$ y $f_u(\tau) = \tau(u) - u$. Aplicando a esta última ecuación σ se obtiene $\sigma(f(\tau)) = \sigma(\tau(u)) - \sigma(u)$. Al sumar esta ecuación con la primera se obtiene que f_u es un homomorfismo cruzado. Notemos de paso que si $\sigma \in G$ entonces $f_u(\sigma) = \sigma(u) - u$ está en $\mu(L)$, puesto que existe un $N \in R_T$ tal que $u^N \in \mathcal{K}$ por lo tanto $(\sigma(u) - u)^N = (\sigma(u))^N - u^N = \sigma(u^N) - u^N = 0$.

Además $\theta(u+v) = f_{u+v}$ y $f_{u+v}(\sigma) = \sigma(u+v) - (u+v) = \sigma(u) + \sigma(v) - u - v = \sigma(u) - u + \sigma(v) - v$, es decir, $\theta(u+v) = \theta(u) + \theta(v)$. Por lo tanto θ es un homomorfismo. Por otra parte, sea $u \in \text{núc}(\theta)$. Así $\theta(u) = f_u = 0$, es decir, $f_u(\sigma) = \sigma(u) - u = 0$, y como L/\mathcal{K} es de Galois, entonces $u \in \mathcal{K}$.

Recíprocamente si $u \in \mathcal{K}$, ciertamente $\theta(u) = 0$. Así $\text{núc}(\theta) = \mathcal{K}$ y por lo tanto tenemos un monomorfismo de grupos abelianos

$$\phi : \text{cog}(L/\mathcal{K}) \rightarrow Z^1(G, \mu(L)).$$

Por otro lado $Z^1(G, \mu(L)) \subseteq Z^1(G, L)$ y por el Teorema 90 de Hilbert aditivo, se tiene que

$$Z^1(G, L) = B^1(G, L) = \{f \in Z^1(G, L) \mid \text{existe un } u \in L \text{ tal que } f = f_u\}.$$

Entonces, dado $f \in Z^1(G, \mu(L))$ existe un $u \in L$ tal que $f = f_u$, por lo que para cada $\sigma \in G$, $f(\sigma) = f_u(\sigma) = \sigma(u) - u \in \mu(L)$. Ahora, u es algebraico sobre \mathcal{K} , y se puede considerar la cerradura de Galois \mathcal{K}' de $\mathcal{K}(u)/\mathcal{K}$. Se tiene que $\mathcal{K} \subseteq \mathcal{K}(u) \subseteq \mathcal{K}' \subseteq L$.

Sea $H = \text{Gal}(L/\mathcal{K}')$. Entonces $H \triangleleft G$ y $\text{card}(G/H)$ es finita. Los conjugados de u son $\{\bar{\sigma}(u) \mid \bar{\sigma} \in \bar{G} = G/H\}$, así

$$\bar{\sigma}(u) = \sigma(u) = u + z_\sigma \text{ con } z_\sigma \in \mu(L).$$

Ahora bien, puesto que únicamente hay un número finito de elementos $\bar{\sigma} \in \bar{G} = \{\sigma_1 H, \dots, \sigma_s H\}$ existen $N_{\sigma_1}, \dots, N_{\sigma_s} \in R_T$ tales que $(z_{\sigma_i})^{N_{\sigma_i}} = 0$, sea $N = N_{\sigma_1} \cdots N_{\sigma_s}$ entonces

$$\bar{\sigma}(u^N) = (u + z_\sigma)^N = u^N + z_\sigma^N = u^N + (z_\sigma^{N_\sigma})^{P_\sigma} = u^N.$$

Como la extensión \mathcal{K}'/\mathcal{K} es de Galois, esto implica que $u^N \in \mathcal{K}$, es decir, ϕ es suprayectiva. \square

Del Teorema 10.6.4, obtenemos el siguiente resultado.

Proposición 10.6.5. *Sean E/F una extensión finita de Galois con grupo de Galois $\Gamma = \text{Gal}(E/F)$ y Δ un subgrupo normal de Γ . Entonces la sucesión canónica de grupos abelianos*

$$0 \rightarrow Z^1(\Gamma/\Delta, \mu(E/F)^\Delta) \xrightarrow{\theta_1} Z^1(\Gamma, \mu(E/F)) \xrightarrow{\theta_2} Z^1(\Delta, \mu(E/F))$$

es exacta, donde $\mu(E/F)^\Delta = \{\zeta \in \mu(E/F) \mid \sigma(\zeta) = \zeta \forall \sigma \in \Delta\}$.

Demostración. Supongamos que $\theta_1(f) = 0$. Entonces si $\bar{\sigma} \in \Gamma/\Delta$, se tiene que $f(\bar{\sigma}) = \theta_1(f)(\sigma) = 0$. De este modo θ_1 es inyectiva. Por otro lado $\text{im}(\theta_1) \subseteq \text{nuc}(\theta_2)$ ya que si $f = \theta_1(f')$, con $f' \in Z^1(\Gamma/\Delta, \mu(E/F)^\Delta)$, entonces $\theta_2(f)(\sigma) = \theta_1(f')(\sigma) = f'(\bar{\sigma}) = 0$.

Ahora si $f \in \text{nuc}(\theta_2)$ entonces para cada $\sigma \in \Delta$, se tiene que $f(\sigma) = 0$. Por lo se puede definir $f' : \Gamma/\Delta \rightarrow \mu(E/F)$ mediante $f'(\bar{\sigma}) = f(\sigma)$. Por la condición impuesta a f , f' esta bien definida y es un morfismo cruzado. Finalmente si $\tau \in \Delta$ entonces $\tau(f'(\bar{\sigma})) = \tau(f(\tau^{-1} \circ \sigma)) = \tau(f(\sigma)) = f'(\bar{\sigma})$, es decir, $f' \in Z^1(\Gamma/\Delta, \mu(E/F)^\Delta)$ y $f = \theta_1(f')$. \square

Corolario 10.6.6. *Sea L/\mathcal{K} una extensión de Galois finita. Si la cardinalidad de $\mu(L)$ es finita entonces el R_T -módulo $\text{cog}(L/\mathcal{K})$ es finito.*

Demostración. Se sigue de la Proposición 10.6.4. \square

10.7. Algunos teoremas de estructura de extensiones radicales ciclotómicas

Proposición 10.7.1. *Sea L/\mathcal{K} una extensión de campos, tal que $[L : \mathcal{K}] = \ell$ con ℓ un primo diferente a $p = \text{car}(\mathcal{K})$. Entonces L/\mathcal{K} no es radical ciclotómica.*

Demostración. Supongamos que L/\mathcal{K} es radical ciclotómica, por lo tanto $\text{cog}(L/\mathcal{K})$ es no trivial. Sea $\bar{\alpha} \in \text{cog}(L/\mathcal{K})$ distinto de 0, esto significa que $\alpha \notin \mathcal{K}$. Así, existe un $M \in R_T$ tal que $\alpha^M \in \mathcal{K}$. Podemos suponer que M es mónico y que es el polinomio de grado mínimo con tal propiedad, es decir, el orden de $\bar{\alpha}$ es M . Por lo que es posible suponer que existe un polnomio irreducible Q , reemplazando a α si es necesario, tal que $\alpha^Q = a \in \mathcal{K}$.

Sea $f(X) = \text{Irr}(\alpha, X, \mathcal{K}) \in \mathcal{K}[X]$, puesto que $\alpha^Q - a = 0$ entonces $f(X) \mid X^Q - a$. Por lo tanto $f(X) = \prod (X - (\alpha + \lambda_Q^B))$, para ciertos $B \in R_T$. Observemos que $\text{gr}(f(X)) = \ell$, pues $L = \mathcal{K}(\alpha)$ y por lo tanto $\sum (\alpha + \lambda_Q^B) = \ell\alpha + \lambda_Q^{\sum B} \in \mathcal{K}$. Por otro lado, puesto que $\ell \neq p$ entonces $\ell \neq 0$ en \mathcal{K} . Así pues $D = \sum B$ es diferente de cero pues, en caso contrario, tendríamos que $\alpha \in \mathcal{K}$ por lo que podemos suponer que el grado de D es menor que el grado de Q .

Por otra parte $\lambda_Q^D \notin \mathcal{K}$, pero $\lambda_Q^D \in L$ y, por pureza, $\lambda_Q^D \in \mathcal{K}$, lo cual es una contradicción. Por lo tanto L/\mathcal{K} no es una extensión radical ciclotómica. \square

Corolario 10.7.2. *Sea L/\mathcal{K} una extensión de Galois, tal que $[L : \mathcal{K}] = p^s n$, con $p \nmid n$, $n > 1$ y $p = \text{car}(\mathcal{K})$. Entonces L/\mathcal{K} no es una extensión radical ciclotómica.*

Demostración. Por el teorema de Cauchy el grupo $G = \text{Gal}(L/\mathcal{K})$ tiene un elemento de orden ℓ , digamos g , donde ℓ es un primo que divide a n . Considere el subgrupo $H = \langle g \rangle$ de G . Si L/\mathcal{K} fuese radical ciclotómica entonces, por la Proposición 10.6.2, la extensión L/L' , donde $L' = L^H$, sería radical ciclotómica. Pero $[L : L'] = \ell$ y por la Proposición 10.7.1 tal extensión no es radical ciclotómica. Por lo tanto L/\mathcal{K} no es radical ciclotómica. \square

Corolario 10.7.3. *Si L/\mathcal{K} es Galois y radical ciclotómica, entonces $[L : \mathcal{K}]$ es de la forma p^s , con $s \in \mathbb{N}$ y $p = \text{car}(\mathcal{K})$.*

Demostración. Si ocurre lo contrario, se tendrá que $[L : \mathcal{K}] = p^n m$, con n entero y ≥ 0 , $p \nmid m$ y $m > 1$. Sin embargo por el Corolario 10.7.2 L/\mathcal{K} no sería radical ciclotómica, lo cual es una contradicción. \square

Lema 10.7.4. *Sea L/\mathcal{K} una extensión tal que $[L : \mathcal{K}] = p^s$ con $s \in \mathbb{N}$ y $p = \text{car}(\mathcal{K})$. Entonces L/\mathcal{K} es pura.*

Demostración. Supongamos que L/\mathcal{K} no es pura, así existe un $a = \lambda_P \in L$, un $P \in R_T$ irreducible tal que $a^P = 0$ pero $a \notin \mathcal{K}$. Considere el diagrama siguiente

$$\begin{array}{ccc} & & L \\ & & \downarrow \\ K(\lambda_P) & \text{---} & K(\lambda_P)\mathcal{K} = \mathcal{K}(\lambda_P) \\ \downarrow & & \downarrow \\ K & \text{---} & \mathcal{K} \end{array}$$

Sea $\widetilde{\mathcal{K}} = \mathcal{K} \cap K(\lambda_P)$. Entonces, por Teoría de Galois, se tiene que $\mathcal{K}(\lambda_P)/\widetilde{\mathcal{K}}$ es Galois, con grupo de Galois G isomorfo a $\text{Gal}(K(\lambda_P)/\widetilde{\mathcal{K}})$. Por otro lado

$$|G| \parallel [L : \mathcal{K}] = p^s \quad \text{y} \quad |G| \parallel (q^d - 1)$$

donde $d = \text{gr}(P)$. Por lo tanto $|G| = 1$, es decir, $\lambda_P \in \mathcal{K}$. \square

Ejemplo 10.7.5. Una extensión de *Carlitz–Kummer*, ver [66], es una extensión L/\mathcal{K} tal que

- (1) \mathcal{K} es una extensión finita de $K(A_M)$, para algún $M \in R_T$.
- (2) L es campo de descomposición del polinomio $f(X) = X^M - z \in \mathcal{K}[u]$, sobre \mathcal{K} , donde $z \in \mathcal{K} \setminus \mathcal{K}^M$.

Por el Teorema 10.4.3, se tiene que $[L : \mathcal{K}] = p^t$, donde $p = \text{car}(\mathcal{K})$. Ahora el Lema 10.7.4 muestra que las extensiones de Carlitz Kummer son extensiones radicales ciclotómicas.

Por otro lado, en base a los resultados anteriores, se tiene el siguiente teorema.

Teorema 10.7.6. *Una extensión, de Galois, L/\mathcal{K} es radical ciclotómica si y sólo si es radical, separable y $[L : \mathcal{K}] = p^s$ con $s \in \mathbb{N}$ y $p = \text{car}(\mathcal{K})$. \square*

En este contexto se tiene el siguiente teorema.

Teorema 10.7.7. *Si L/\mathcal{K} es radical ciclotómica, entonces $[L : \mathcal{K}] = p^n$ para alguna $n \geq 0$, donde $p = \text{car}(\mathcal{K})$.*

Demostración. Sea L/\mathcal{K} una extensión radical ciclotómica. Entonces $L = \mathcal{K}(\alpha_1, \dots, \alpha_t)$ de tal modo que $\alpha_i^{M_i} = a_i \in \mathcal{K}$ donde $M_i \in R_T$. Entonces

$$[L : \mathcal{K}] = [L : \mathcal{K}(\alpha_1, \dots, \alpha_{t-1})] \cdots [\mathcal{K}(\alpha_1, \alpha_2) : \mathcal{K}(\alpha_1)][\mathcal{K}(\alpha_1) : \mathcal{K}].$$

Puesto que cada $\mathcal{K}(\alpha_1, \dots, \alpha_i)/\mathcal{K}(\alpha_1, \dots, \alpha_{i-1})$ es una extensión finita radical ciclotómica, es suficiente considerar el caso $L = \mathcal{K}(\alpha)$.

Supongamos que $L = \mathcal{K}(\alpha)$ con $\alpha^M \in \mathcal{K}$ para algún $M \in R_T$. Sea $M = P_1^{e_1} \cdots P_s^{e_s}$ su factorización como producto de polinomios irreducibles distintos. Sea $\beta_j := \alpha^{M/P_j^{e_j}}$ para $1 \leq j \leq s$. Se tiene que $L = \mathcal{K}(\beta_1, \dots, \beta_s)$. Por el mismo argumento anterior, podemos suponer $L = \mathcal{K}(\alpha)$ con $\alpha^{P^e} \in \mathcal{K}$ para algún polinomio irreducible $P \in R_T$.

Ahora sea $L = \mathcal{K}(\alpha)$ tal que $\alpha^{P^e} \in \mathcal{K}$ para algún polinomio irreducible $P \in R_T$. Sean $\gamma_i = \alpha^{P^{e-i}}$ para $1 \leq i \leq e$. Entonces $\mathcal{K} \subseteq \mathcal{K}(\gamma_1) \subseteq \mathcal{K}(\gamma_2) \subseteq \cdots \subseteq \mathcal{K}(\gamma_e) = L$. Por lo tanto

$$[L : \mathcal{K}] = [L : \mathcal{K}(\gamma_{e-1})] \cdots [\mathcal{K}(\gamma_2) : \mathcal{K}(\gamma_1)][\mathcal{K}(\gamma_1) : \mathcal{K}].$$

Puesto que cada $\mathcal{K}(\gamma_i)/\mathcal{K}(\gamma_{i-1})$ es una extensión radical ciclotómica, es suficiente considerar el caso $L = \mathcal{K}(\alpha)$ con $\alpha^P \in \mathcal{K}$ para algún polinomio irreducible $P \in R_T$.

Supongamos $\lambda_P \in L$. Entonces L/\mathcal{K} es de Galois por ser el campo de descomposición de $X^P - \alpha^P \in \mathcal{K}[X]$. Por el Corolario 10.7.3, L/\mathcal{K} es una p -extensión.

Ahora supongamos que $\lambda_P \notin L$. Consideremos el diagrama

$$\begin{array}{ccccc} L = \mathcal{K}(\alpha) & \xrightarrow{a} & L(\lambda_P) = \mathcal{K}(\lambda_P, \alpha) & & \\ & & \downarrow b & & \downarrow b \\ \mathcal{K} & \xrightarrow{d} & \mathcal{K}(\alpha) \cap \mathcal{K}(\lambda_P) & \xrightarrow{a} & \mathcal{K}(\lambda_P) \\ & & \downarrow c & & \downarrow c \\ K & \xrightarrow{d} & \mathcal{K} \cap K(\lambda_P) & \xrightarrow{d} & \mathcal{K}(\alpha) \cap K(\lambda_P) & \xrightarrow{a} & K(\lambda_P) \end{array}$$

Puesto que $\mathcal{K}(\lambda_P, \alpha)/\mathcal{K}(\lambda_P)$ es Galois además, por el Teorema 10.4.3 se tiene que $N = \text{Gal}(L(\lambda_P)/\mathcal{K}(\lambda_P))$ puede considerarse como un subgrupo de Λ_P , es decir, N es un p -grupo elemental abeliano y $|N| = b = p^n$.

Puesto que

$$[L : \mathcal{K}] = [L : \mathcal{K}(\alpha) \cap \mathcal{K}(\lambda_P)][\mathcal{K}(\alpha) \cap \mathcal{K}(\lambda_P) : \mathcal{K}] = bd = p^n d$$

basta mostrar que $d = 1$.

Sean $H = \text{Gal}(L(\lambda_P)/(\mathcal{K}(\alpha) \cap \mathcal{K}(\lambda_P)))$, $G = \text{Gal}(L(\lambda_P)/\mathcal{K})$ y $N = \text{Gal}(L(\lambda_P)/\mathcal{K}(\lambda_P))$. Nótese que N es un subgrupo normal de G .

Se tiene que

$$G/N \cong \text{Gal}(\mathcal{K}(\lambda_P)/\mathcal{K}) < \text{Gal}(K(\lambda_P)/K) \cong C_{q^d-1}.$$

Así pues G/N es un grupo cíclico de orden $q^d - 1$, en particular, primo relativo a p . Además se tiene que $|G/N| = ad$.

Por el Teorema de Hall, ver [19] Teorema 9.3.1, como G es soluble, existe un subgrupo R de G con R cíclico de orden ad , tal que $G = NR$ (de hecho G es el producto semidirecto $G \cong N \rtimes R$ ya que $(|R|, |N|) = 1$).

Por el mismo Teorema de Hall, todo subgrupo de orden un divisor de $|R| = ad$ esta contenido en un conjugado R' de R y se tiene que $G = NR' \cong N \rtimes R'$.

Sea $S = \text{Gal}(L(\lambda_P)/\mathcal{K}(\alpha)) \cong C_a$. Por lo tanto podemos suponer $S \subseteq R$ y $|R/S| = d$. Notemos que $(d, p) = 1$.

Sea $E = L(\lambda_P)^R$. Observemos que $L(\lambda_P)^S = \mathcal{K}(\alpha) = L$. Por lo tanto $\mathcal{K} \subseteq E \subseteq L$, $[L : E] = [R : S] = d = |R/S|$. Ahora, como L/\mathcal{K} es una extensión radical ciclotómica lo es también L/E . Por lo tanto $d = 1$. \square

Corolario 10.7.8. *Con las notaciones del Teorema 10.7.7 tenemos $\mathcal{K}(\alpha) \cap \mathcal{K}(\lambda_P) = \mathcal{K}$, $[L : \mathcal{K}] = [L(\lambda_P) : \mathcal{K}(\lambda_P)]$. Además*

$$\text{Irr}(\alpha, X, \mathcal{K}) = \text{Irr}(\alpha, X, \mathcal{K}(\lambda_P)) = F_1(X) = \prod (X - (\alpha + \lambda_P^A)).$$

Demostración. Se sigue de la demostración del Teorema 10.7.7. \square

Corolario 10.7.9. *Una extensión finita L/\mathcal{K} es radical ciclotómica si y sólo si es separable, radical y $[L : \mathcal{K}] = p^m$ para algún $m \in \mathbb{N}$.*

Demostración. Se sigue del Teorema 10.7.7 y del Lema 10.7.4. \square

10.8. Ejemplos y aplicaciones

En esta sección veremos algunas aplicaciones de los resultados anteriores. En primer lugar tenemos la siguiente consecuencia del Teorema 10.6.4.

Corolario 10.8.1. *Si E/L es una extensión finita y de Galois, con grupo de Galois Γ , entonces la función:*

$$\phi : \{H \mid L \leq H \leq T(E/L)\} \rightarrow \{U \mid U \leq Z^1(\Gamma, \mu(E))\},$$

dada por $\phi(H) = \{f_\alpha \in Z^1(\Gamma, \mu(E)) \mid \alpha \in H\}$, es un isomorfismo de redes.

Demostración. Se sigue del isomorfismo dado en el Teorema 10.6.4. \square

Ahora, sea E/L una extensión de Galois con grupo de Galois Γ . Definimos

$$f : \text{Gal}(E/L) \times \text{cog}(E/L) \rightarrow \mu(E)$$

dado por $f(\sigma, \bar{u}) = \sigma(u) - u$. Puesto que $\text{cog}(E/L) \rightarrow Z^1(\Gamma, \mu(E))$ es un isomorfismo, se tiene la función evaluación

$$\langle, \rangle : \Gamma \times Z^1(\Gamma, \mu(E)) \rightarrow \mu(E)$$

dado por $\langle \sigma, h \rangle = h(\sigma)$.

Ahora para cada $\Delta \leq \Gamma$, $U \leq Z^1(\Gamma, \mu(E))$ y $\chi \in Z^1(\Gamma, \mu(E))$ definimos:

$$\Delta^\perp = \{h \in Z^1(\Gamma, \mu(E)) \mid \langle \sigma, h \rangle = 0 \text{ para cada } \sigma \in \Delta\},$$

$$U^\perp = \{\sigma \in \Gamma \mid \langle \sigma, h \rangle = 0 \text{ para cada } h \in U\},$$

$$\chi^\perp = \{\sigma \in \Gamma \mid \langle \sigma, \chi \rangle = 0\}.$$

Así $\Delta^\perp \leq Z^1(\Gamma, \mu(E))$ y $U^\perp \leq \Gamma$.

Proposición 10.8.2. *Sea E/L una extensión finita y de Galois con grupo de Galois Γ . Sea L' una extensión intermedia de E/L . Entonces L'/L es radical si y solamente si existe un subgrupo $U \leq Z^1(\Gamma, \mu(E))$ tal que $\text{Gal}(E/L') = U^\perp$.*

Demostración. Si L'/L es una extensión radical, existe $\tilde{G} \subseteq T(E/L)$ tal que $L' = L(\tilde{G})$. Podemos reemplazar \tilde{G} por el subgrupo *aditivo* generado por \tilde{G} y L , que denotamos por G . Así $L \leq G \leq T(E/L)$ y $L' = L(G)$. Sea

$$U = \phi(G) = \{f_\alpha \mid \alpha \in G\} \leq Z^1(\Gamma, \mu(E))$$

donde ϕ es la función dada en el Corolario 10.8.1. Entonces

$$\begin{aligned} U^\perp &= \{\sigma \in \Gamma \mid \langle \sigma, f_\alpha \rangle = 0 \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid f_\alpha(\sigma) = 0 \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid \sigma(\alpha) = \alpha \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid \sigma(x) = x \text{ para cada } x \in L(G)\} \\ &= \text{Gal}(E/L(G)) = \text{Gal}(E/L'). \end{aligned}$$

Recíprocamente, en caso de que exista un subgrupo $U \leq Z^1(\Gamma, \mu(E))$ tal que $\text{Gal}(E/L') = U^\perp$, entonces veamos que

$$\text{Gal}(E/L') = U^\perp = \text{Gal}(E/L(G)),$$

con $G = \{\alpha \in E \mid f_\alpha \in U\} = \phi^{-1}(U)$ donde ϕ es la función dada en el Corolario 10.8.1.

Para mostrar las igualdades anteriores sólo debemos mostrar $U^\perp = \text{Gal}(E/L(G))$. Para este fin consideremos $\tau \in U^\perp = \{\sigma \in \Gamma \mid h(\sigma) = 0 \forall h \in U\}$. Ahora si $\alpha \in G$ entonces $f_\alpha \in U$, en particular, $f_\alpha(\tau) = 0 = \tau(\alpha) - \alpha$. Por lo tanto para todo $\alpha \in G$, $\tau(\alpha) = \alpha$ y, de este modo, τ fija a $L(G)$ así que $\tau \in \text{Gal}(E/L(G))$.

Ahora si $\tau \in \text{Gal}(E/L(G))$, sea $h \in U$. Entonces existe un $\alpha \in G$ tal que $h = f_\alpha$, por la definición de G y el hecho de que ϕ es biyectiva. Se sigue que $h(\tau) = f_\alpha(\tau) = 0$ por lo que $\tau \in U^\perp$. Ahora por Teoría de Galois, se tiene que $L' = L(G)$ \square

El siguiente resultado es una aplicación de la Proposición 10.8.2, ver [7]. El símbolo $\sqrt[N]{\alpha}$ denota una raíz del polinomio $u^N - \alpha$.

Proposición 10.8.3. Sean \mathcal{K}/F una extensión finita y separable y E la cerradura normal de \mathcal{K}/F . Supongamos que existe una extensión finita L/F tal que

- (1) $E(\lambda_N) \cap L = F$ donde $N \in R_T$ es un polinomio no constante.
 - (2) $\mathcal{K}L = L(\sqrt[N]{\alpha})$ para algún $\alpha \in L$ distinto de 0.
- Entonces $\mathcal{K} = F(\sqrt[N]{\alpha})$.

Demostración. Consideremos el diagrama siguiente

$$\begin{array}{ccc}
 E(\lambda_N) & \text{---} & E(\lambda_N)L \\
 \downarrow & & \downarrow \\
 \mathcal{K} & \text{---} & \mathcal{K}L \\
 \downarrow & & \downarrow \\
 F & \text{---} & L
 \end{array}$$

Puesto que la extensión $E(\lambda_N)/F$ es de Galois se tiene que $E(\lambda_N)L/L$ es una extensión de Galois y de la hipótesis (1) se tiene

$$G = \text{Gal}(E(\lambda_N)/F) \cong \text{Gal}(E(\lambda_N)L/L) = G_1.$$

Por la hipótesis (2) se tiene $\mathcal{K}L = L(\sqrt[N]{\alpha})$. Sea $\beta = \sqrt[N]{\alpha}$ y considere $\sigma \in \text{Gal}(E(\lambda_N)L/\mathcal{K}L)$. Entonces

$$(\sigma(\beta) - \beta)^N = \sigma(\beta^N) - \beta^N = \sigma(\alpha) - \alpha = 0. \quad (10.7)$$

Por lo tanto definimos $\chi : G_1 \rightarrow \mu(E(\lambda_N)L)$ por $\chi(\sigma) = \sigma(\beta) - \beta$.

Entonces $\text{Gal}(E(\lambda_N)L/\mathcal{K}L) = \text{núc}(\chi)$, ya que si $\sigma \in \text{Gal}(E(\lambda_N)L/\mathcal{K}L)$ se tiene que $\chi(\sigma) = \sigma(\beta) - \beta = 0$ y recíprocamente. Además, de (10.7) se tiene que χ toma valores en A_N . Puesto que G y G_1 son isomorfos, χ puede ser definido en G .

Por lo anterior χ puede considerarse como un elemento de $Z^1(G, E(\lambda_N))$ y $\text{núc}(\chi)$ es igual a $\text{Gal}(E(\lambda_N)/\mathcal{K})$, puesto que G y G_1 es isomorfo. Por la Proposición 10.8.2 \mathcal{K}/F es una extensión radical. \square

Sea E/F una extensión finita de Galois, con grupo de Galois G . Sea L/F otra extensión tal que $L \cap E = F$, considere la composición EL . La función de restricción

$$\text{Gal}(EL/L) \rightarrow \text{Gal}(E/F), \quad \sigma \mapsto \sigma|_E$$

es un isomorfismo de grupos. Denotamos por $S(L_1/L_2)$ al subconjunto de extensiones de L_1 contenidas en L_2 . Entonces las funciones

$$\varepsilon : S(E/F) \rightarrow S(EL/L), \quad \mathcal{K}'/F \mapsto L\mathcal{K}'/L$$

y

$$\lambda : S(EL/L) \rightarrow S(E/F), \quad \mathcal{K}_1/L \mapsto (\mathcal{K}_1 \cap E)/F$$

son isomorfismo de redes, inversas una de la otra.

Denotamos por $ST(E/F)$ al conjunto de todas las subextensiones \mathcal{K}'/F de E/F que son radicales. Entonces para todo $\mathcal{K}'/F \in ST(E/F)$ existe un R_T -módulo G , no necesariamente único, tal que $F \subseteq G \subseteq T(E/F)$ y $\mathcal{K}' = F(G)$. Definimos $G_1 = G + L$. Entonces $L\mathcal{K}' = L(G_1)$, ya que $L\mathcal{K}' = L(G)$, $L \subseteq G_1 \subseteq T(EL/L)$ y G_1 es un R_T -módulo. Por tanto $\varepsilon(\mathcal{K}'/L) \in ST(EL/L)$. De este modo la restricción de ε a las extensiones radicales da lugar a una función inyectiva

$$\rho : ST(E/F) \rightarrow ST(EL/L)$$

definida por

$$F(G)/F \mapsto F(G)L/L = L(G + L)/L$$

donde G es un R_T -módulo tal que $F \subseteq G \subseteq T(E/F)$.

Proposición 10.8.4. *Sea E/F una extensión finita de Galois con grupo de Galois Γ y sea L/F una extensión arbitraria, con $L \subseteq \overline{K}$, tal que $E \cap L = F$. Si $\mu(EL) = \mu(E)$, entonces se tiene:*

- (1) $(G + L) \cap E = G$ para todo R_T -módulo G con $F \subseteq G \subseteq T(E/F)$.
- (2) $G_1 = (G_1 \cap E) + L$ para todo R_T -módulo G_1 , con $L \subseteq G_1 \subseteq T(EL/L)$.
- (3) La función

$$\begin{aligned} \rho : ST(E/F) &\rightarrow ST(EL/L) \\ F(G)/F &\mapsto L(G + L)/L, \quad F \leq G \leq T(E/F) \end{aligned}$$

es biyectiva, y la función

$$\begin{aligned} ST(EL/L) &\rightarrow ST(E/F), \\ L(G_1)/L &\mapsto F(G_1 \cap E)/F, \quad L \leq G_1 \leq T(EL/L) \end{aligned}$$

es su inversa.

Aquí, la notación $F \leq G$ indica que F es un submódulo del R_T -módulo G .

Demostración. (1) Sea $w \in (G + L) \cap E$ así $w = x + y$ donde $x \in G$ e $y \in L$, por lo que $y = w - x \in E$. Así $y \in F$ ya que $E \cap L = F$. Por lo tanto $w \in G$.

Recíprocamente si $x \in G$ ciertamente $x \in (G + L) \cap E$.

(2) Denotamos por Γ_1 al grupo de Galois de EL/L . Hemos visto anteriormente que se tiene un isomorfismo de grupos

$$\Gamma_1 \rightarrow \Gamma, \quad \sigma_1 \rightarrow \sigma_1|_E \quad (10.8)$$

Como $\mu(EL) = \mu(E)$, el isomorfismo anterior induce un isomorfismo de grupos

$$v : Z^1(\Gamma, \mu(E)) \rightarrow Z^1(\Gamma_1, \mu(EL))$$

dado como sigue: sea $h \in Z^1(\Gamma, \mu(E))$. Si $\sigma_1 \in \Gamma_1$ se tiene que $\sigma_1|_E \in \Gamma$, y definimos $v(h)(\sigma_1) := h(\sigma_1|_E)$. Ahora

$$v(h)(\sigma_1 \circ \sigma_2) = h(\sigma_1 \circ \sigma_2|_E) = h(\sigma_1|_E \circ \sigma_2|_E).$$

Así $v(h)$ es un homomorfismo cruzado. Por construcción v es un homomorfismo de grupos, y por (10.8) se tiene el que v es un isomorfismo de grupos.

Sea G_1 con $L \leq G_1 \leq T(EL/L)$. Ahora si $w \in (G_1 \cap E) + L$ entonces $w = x + y$ con $x \in (G_1 \cap E)$ e $y \in L$, así $w \in G_1$. Ahora sea $a_1 \in G_1$. Entonces $f_{a_1} \in Z^1(\Gamma_1, \mu(EL))$. Tenemos que existe $f \in Z^1(\Gamma, \mu(E))$ tal que $f_{a_1} = v(f)$. De la Proposición 10.6.4, existe $a \in T(E/F)$ tal que $f_{a_1} = v(f = f_a)$.

Se tiene que $f_{a_1}(\sigma_1) = f_a(\sigma_1|_E)$ para todo $\sigma_1 \in \Gamma_1$. De aquí se sigue que $\sigma_1(a_1) - a_1 = \sigma_1(a) - a$, es decir, $\sigma_1(a_1 - a) = a_1 - a$ para cada $\sigma_1 \in \Gamma_1$. Así pues $a_1 - a \in L$. Por lo tanto $a_1 = a + b$ donde $b \in L$. Puesto que $a \in G_1$ se sigue que $a \in (G_1 \cap E) + L$.

(3) Por la observación hecha previamente a esta proposición se tiene que ρ es inyectiva, por lo que basta mostrar que ρ es suprayectiva. Para ello, sea $\mathcal{K}_1/L \in ST(EL/L)$. Entonces $\mathcal{K}_1 = L(G_1)$ para algún G_1 con $L \leq G_1 \leq T(EL/L)$. Por lo tanto si ponemos $G = G_1 \cap E$, obtenemos que $F(G)/F \in ST(E/F)$ y que

$$\rho(F(G)/F) = L(F(G))/L = L(F(G_1 \cap E))/L = L(L + (G_1 \cap E))/L.$$

Por (2), se tiene que $L(L + (G_1 \cap E)) = L(L + G) = L(G_1) = \mathcal{K}_1$. \square

Por otro lado, el recíproco del Teorema 10.7.7 no siempre es válido como lo muestra el siguiente lema.

Lema 10.8.5. Sea L/\mathcal{K} una extensión Galois tal que $[L : \mathcal{K}] = p^2$, $\mu(L) = \mu(\mathcal{K})$ y $G = \text{Gal}(L/\mathcal{K}) \cong C_{p^2}$. Entonces L/\mathcal{K} no es una extensión radical.

Demostración. Supongamos que la extensión L/\mathcal{K} es radical. Considere el grupo $H^1(G, \mu(L))$. Puesto que $\mu(L) = \mu(\mathcal{K})$ se tiene que $B^1(G, \mu(L)) = \{1\}$. Por tanto, $H^1(G, \mu(L)) = Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong \text{Hom}(G, \mu(L))$. En consecuencia, por la Proposición 10.6.4, se tendrá

$$\text{cog}(L/\mathcal{K}) \cong \text{Hom}(G, \mu(\mathcal{K})).$$

Consideremos un elemento de orden p , digamos τ , en G . Sea $H = \langle \tau \rangle$ y $L' = L^H$. Notemos que, al ser H normal en G , se tiene que L'/\mathcal{K} es una extensión normal y, por lo tanto, de Galois. Además $G' = \text{Gal}(L'/\mathcal{K})$ es isomorfo a C_p . Nótese que $\mu(L') = \mu(\mathcal{K})$. Así

$$\text{cog}(L'/\mathcal{K}) \cong \text{Hom}(G', \mu(\mathcal{K})).$$

Notemos que la cardinalidad de $\text{cog}(L/\mathcal{K}) \cong \text{Hom}(G, \mu(\mathcal{K}))$ es $|\mu(\mathcal{K})|$. Para ver esto sea $a \in G \cong C_{p^2}$ un generador. Un homomorfismo $\psi : G \rightarrow \mu(\mathcal{K})$ queda completamente determinado por su acción en a . Por lo tanto hay $|\mu(\mathcal{K})|$ homomorfismos de G en $\mu(\mathcal{K})$. Del mismo modo podemos mostrar que la cardinalidad de $\text{cog}(L'/\mathcal{K}) \cong \text{Hom}(G', \mu(\mathcal{K}))$ es $|\mu(\mathcal{K})|$.

Por otro lado tenemos que $\text{cog}(L'/\mathcal{K}) \subseteq \text{cog}(L/\mathcal{K})$, ver Proposición 10.6.2. Entonces, como ambos grupos tienen la misma cardinalidad, se tiene $\text{cog}(L'/\mathcal{K}) = \text{cog}(L/\mathcal{K})$. Se sigue que $L = L'$, ya que si $\alpha_1, \dots, \alpha_s$ generan a L sobre \mathcal{K} , entonces por lo mostrado se tendrá que $\alpha_1, \dots, \alpha_s \in L'$ y de aquí la afirmación. Se tendría que $[L : \mathcal{K}] = p^2 = [L' : \mathcal{K}] = p$ lo cual es una contradicción. \square

El siguiente ejemplo muestra que la propiedad de ser extensión radical no es hereditaria.

Ejemplo 10.8.6. Sea $M = P^n$, $n \in \mathbb{N}$ y $P \in R_T$ irreducible, se considera la extensión $K(\Lambda_M)/K(\lambda_P)$. Sea $t \in \mathbb{N}$ de tal modo que $p^{t-1} < n \leq p^t$ y n_0 la parte entera de $\frac{n}{p^{t-1}}$.

Del Corolario 1 de [40], se obtiene

$$H_M \cong (\mathbb{Z}/p^t\mathbb{Z})^\alpha \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_s}\mathbb{Z}$$

con $t > n_1 \geq \dots \geq n_s \geq 0$. Aquí H_M es el grupo de Galois de la extensión $k(\Lambda_M)/k(\lambda_P)$.

Sea $n = 5$ y $p = 3$. Si $t = 2$ se cumple que $p^{t-1} < n \leq p^t$. Además $n_0 = 1$. El valor de α está dado por el Corolario 1 de [40].

Se puede escoger un subgrupo de H_M de la forma

$$H_M = (\mathbb{Z}/p^t\mathbb{Z})^{\alpha-1} \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_s}\mathbb{Z}.$$

Sea $L' = L^H$, así $\text{Gal}(L'/K(\lambda_P)) \cong C_{p^2}$. Se tiene también que $\mu(K(\lambda_P)) = \mu(L')$, esto es posible, escogiendo adecuadamente $q = p^\nu$.

Por el Lema 10.8.5, $L'/K(\lambda_P)$ no es radical. Por lo tanto $K(\lambda_{P^5})/K(\lambda_P)$ es una extensión Galois radical ciclotómica, pero no cumple la propiedad de que si L es un campo tal que $K(\lambda_P) \subseteq L \subseteq K(\lambda_{P^5})$, entonces $L/K(\lambda_P)$ es una extensión radical.

Ejemplo 10.8.7. En este ejemplo tendremos $q = p \geq 3$. Considere la extensión $L/K(\Lambda_T)$, donde L es el campo de descomposición del polinomio

$f(X) = X^T - 1$, con coeficientes en $K(\Lambda_T)$. El grado de esta extensión es $[L : K(\Lambda_T)] = p$, ver Ejemplo 10.4.5. Trataremos de determinar la estructura de $\text{cog}(L/K(\Lambda_T))$.

Supongamos que $\bar{\beta} \in \text{cog}(L/K(\Lambda_T))$ tiene orden Q^r , con Q mónico irreducible, $r \geq 1$ y $Q \neq T$. Por la Proposición 10.4.1 se tiene que $\lambda_{Q^r} \in L$. Puesto que $\lambda_Q = \lambda_{Q^r}^{Q^{r-1}} \in L$, por pureza se tiene que $\lambda_Q \in K(\Lambda_T)$, pero esto implica que $Q = T$ lo cual es una contradicción. Por lo tanto

$$\text{cog}(L/K(\Lambda_T)) \cong \text{cog}(L/K(\Lambda_T))_T$$

donde $\text{cog}(L/K(\Lambda_T))_T$ es el conjunto de elementos de $\text{cog}(L/K(\Lambda_T))$ cuyo orden es una potencia de T .

Necesitaremos un lema para obtener la cardinalidad de $\text{cog}(L/K(\Lambda_T))$. Para empezar sea $z \in K$, $z \neq 0$, y $N \in R_T$ un polinomio no constante. Consideremos $g(X) = X^N - z \in K(\Lambda_N)[X]$. El campo de descomposición de $g(X)$, sobre K , es de la forma $\mathcal{K} = K(\alpha, \lambda_N)$ donde α es una raíz arbitraria de $g(X)$ y λ_N un generador de Λ_N . Como el polinomio $g(X)$ es separable, la extensión \mathcal{K}/K es de Galois.

Sea $G = \text{Gal}(L/K)$ entonces dado $\sigma \in G$ se tiene que $\sigma(\alpha) = \alpha + \lambda^{M_\sigma}$ y $\sigma(\lambda) = \lambda^{N_\sigma}$, donde M_σ y N_σ se determinan salvo un múltiplo de N , y N_σ es primo relativo a N .

Por otro lado considere $G(N)$ el subgrupo de $GL_2(R_T/(N))$ de todas las matrices de la forma

$$\begin{pmatrix} 1 & 0 \\ \bar{B} & \bar{A} \end{pmatrix}$$

donde $\bar{B} \in R_T/(N)$ y $\bar{A} \in (R_T/(N))^*$. De esta descripción se sigue que $\text{card}(G(N)) = q^{\text{gr}(N)} \Phi(N)$. Sea $\theta : G \rightarrow G(N)$ definida por:

$$\theta(\sigma) = \begin{pmatrix} 1 & 0 \\ \frac{1}{M_\sigma} & \frac{0}{N_\sigma} \end{pmatrix}.$$

Tenemos el siguiente lema.

Lema 10.8.8. *Sea L/K la extensión anteriormente descrita y θ la función anteriormente definida. Entonces θ es un monomorfismo de grupos. Por otra parte si $N = P$, P mónico e irreducible, $z \in R_T$ como antes y la ecuación $g(X) = 0$ no tiene soluciones en R_T , entonces θ es un isomorfismo de grupos.*

Demostración. Sean $\sigma, \tau \in G$. Se tiene que $\sigma(\tau(\alpha)) = \sigma(\alpha + \lambda^{M_\tau}) = \alpha + \lambda^{M_\sigma} + \lambda^{M_\tau N_\sigma}$ además $\sigma(\tau(\lambda)) = \sigma(\lambda^{N_\tau}) = \lambda^{N_\sigma N_\tau}$, por lo tanto

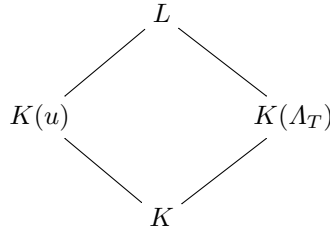
$$\theta(\sigma \cdot \tau) = \begin{pmatrix} 1 & 0 \\ \frac{1}{M_\sigma + M_\tau N_\sigma} & \frac{0}{N_\sigma N_\tau} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{M_\sigma} & \frac{0}{N_\sigma} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{1}{M_\tau} & \frac{0}{N_\tau} \end{pmatrix} = \theta(\sigma)\theta(\tau).$$

Por lo tanto θ es un homomorfismo de grupos. Si $\theta(\sigma)$ es la matriz identidad se tiene que M_σ es un múltiplo de N y que $N_\sigma = 1 + NQ$. Así $\sigma = e$, es decir, θ es un monomorfismo de grupos.

Si $N = P$, donde P es un polinomio mónico e irreducible, $z \in R_T$ como antes y la ecuación $g(X) = 0$ no tiene soluciones en R_T , entonces por el Teorema 1.7 (3) de [29], se tiene que $\text{Gal}(L/K(\lambda_P))$ tiene cardinalidad $q^{\text{gr}(P)}$, es decir, el monomorfismo anterior es un isomorfismo. \square

Regresando a nuestro ejemplo, se mostrará que $\mu(L) = \Lambda_T$. Para empezar, ciertamente $\Lambda_T = \mu(K(\Lambda_T)) \subseteq \mu(L)$. Por otro lado sea $u \in \mu(L)$ no nulo. Existe un $N \in R_T$ tal que $u^N = 0$. Por lo tanto u es de la forma λ_N^M . Podemos suponer que $(M, N) = 1$. Por tanto, por la Proposición 12.2.21 de [70], podemos afirmar que $\lambda_N \in L$. Sea $N = P_1^{\alpha_1} \cdots P_s^{\alpha_s}$. Entonces $\lambda_{P_i} = \lambda_N^{P_1^{\alpha_1} \cdots P_i^{\alpha_i - 1} \cdots P_s^{\alpha_s}} \in L$. Puesto que $L/K(\Lambda_T)$ es pura, tendremos que $\lambda_{P_i} \in K(\Lambda_T)$. Así $P_i = T$. Por lo tanto $N = T^n$ con $n \geq 1$ y $n \in \mathbb{N}$.

Supongamos que $n \geq 2$ y considere el diagrama



Del diagrama anterior obtenemos $[L : K(u)]\Phi(T^n) = p(p-1)$, puesto que $\Phi(T^n) = p^{n-1}(p-1)$, se sigue que $[L : K(u)]p^{n-1} = p$. Si $n \geq 3$ entonces $n-2 \geq 1$, así $[L : K(u)]p^{n-2} = 1$ lo cual es una contradicción. Solo resta considerar el caso $n = 2$, que implica que $L = K(u)$, pero del Lema 10.8.8 se tiene que $\text{Gal}(L/K)$ es un grupo no abeliano, lo cual contradice que el grupo $\text{Gal}(K(\Lambda_{T^2})/K)$ es abeliano. Por lo tanto $n = 1$ y $u = \lambda_T^M \in K(\Lambda_T)$.

Por el Lema 10.9.3 se tiene que $B^1(G, \mu(L)) = \{0\}$. Se sigue $H^1(G, \mu(L)) = Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong \text{Hom}(G, \mu(L))$. De esta manera, utilizando la demostración del Lema 10.8.5, se tiene que

$$|\text{cog}(L/K(\Lambda_T))| = [L : K(\Lambda_T)] = p.$$

Ejemplo 10.8.9. Consideremos la extensión $K(\Lambda_{P^n})/K(\Lambda_P)$. Calcularemos la cardinalidad del módulo $\text{cog}(K(\Lambda_{P^n})/K(\Lambda_P))$ en el siguiente caso: Sea $P(T) = T$, $q = p > 2$ y $n = 2$. Sea $H_{T^2} = \{\overline{N} \in R_T/(T^2) \mid (N, T^2) = 1 \text{ y } N \equiv 1 \pmod{T}\}$. Entonces $\text{card}(H_{T^2}) = q^{d(n-1)} = p$, con $d = \text{gr}(P(T)) = 1$. En particular el grupo H_{T^2} es cíclico. Se tiene que

$$H^1(H_{T^2}, \Lambda_{T^2}) \cong \text{núc}(N_{H_{T^2}})/D\Lambda_{T^2}$$

donde definimos $N_{H_{T^2}} : \Lambda_{T^2} \rightarrow \Lambda_{T^2}$ y $D : \Lambda_{T^2} \rightarrow \Lambda_{T^2}$ como

$$N_{H_{T^2}}(x) = x + \sigma \cdot x + \cdots + \sigma^{p-1} \cdot x,$$

$$D(x) = \sigma \cdot x - x,$$

donde $\sigma = 1 + T + (T^2)$ es un generador de H_{T^2} y $x \in \Lambda_{T^2}$. Por otro lado si $x = \lambda_{T^2}^M$ se tiene que

$$N_{H_{T^2}}(x) = \lambda_{T^2}^M + \lambda_{T^2}^{M(1+T)} + \dots + \lambda_{T^2}^{M(1+(p-1)T)} = \lambda_{T^2}^{pM+(1+2+\dots+p-1)MT} = 0.$$

Notemos que $1 + 2 + \dots + (p-1) = 0$ ya que tal suma es igual a $\frac{p(p-1)}{2} = 0$ en \mathbb{F}_p . De esta manera se tiene que $\text{nuc}(N_{H_{T^2}}) = \Lambda_{T^2}$. Observemos también que $D(x) = \lambda_{T^2}^{M(1+T)} - \lambda_{T^2}^M = \lambda_T^M$. Por tanto

$$D\Lambda_{T^2} = \Lambda_T.$$

Se sigue que $H^1(H_{T^2}, \Lambda_{T^2}) = \Lambda_{T^2}/\Lambda_T$. Por otra parte del Lema 10.9.3 se tiene que $\text{card}(B^1(H_{T^2}, \Lambda_{T^2})) = \text{card}(\Lambda_{T^2}/\Lambda_T)$ y recordando que

$$H^1(H_{T^2}, \Lambda_{T^2}) = Z^1(H_{T^2}, \Lambda_{T^2})/B^1(H_{T^2}, \Lambda_{T^2})$$

se obtiene, por la Proposición 10.6.4,

$$|(\text{cog}(\mathcal{K}(\Lambda_{T^2})/\mathcal{K}(\Lambda_T)))| = |Z^1(H_{T^2}, \Lambda_{T^2})| = [\mathcal{K}(\Lambda_{T^2}) : \mathcal{K}(\Lambda_T)]^2.$$

El siguiente lema, muestra que ciertas extensiones tienen propiedades análogas a las enunciadas en el Lema 1.3 de [18], concretamente los pasos 1 y 2. Sin embargo veremos después que, en general, estas propiedades no se cumplen.

Lema 10.8.10. *Considere la extensión $L/K(\lambda_P)$, donde L es campo de descomposición del polinomio $X^P - a$, donde $P \in R_T$ es irreducible y $a \in K(\lambda_P) \setminus K(\lambda_P)^P$. El módulo $\text{cog}(L/K(\lambda_P))$ no tiene elementos de orden Q , donde Q es un polinomio irreducible, distinto de P . Además si $\nu_{\mathfrak{p}}(a) \geq q^d$, donde $d = \text{gr}(P)$, se tiene que $\text{cog}(L/\mathcal{K})$ no tiene elementos de orden P^2 .*

Demostración. Supongamos que $\text{cog}(L/K(\lambda_P))$ tiene un elemento de orden Q . Entonces como $L/K(\lambda_P)$ es Galois, se tiene que $\lambda_Q \in L$ y como $L/K(\lambda_P)$ es radical ciclotómica, se tendrá que $\lambda_Q \in \mu(\mathcal{K}) = \Lambda_P$, por la Proposición 10.4.1, por lo tanto $Q = P$.

Ahora supongamos que $\text{cog}(L/K(\lambda_P))$ tiene un elemento de orden P^2 , es decir, existe $\hat{\beta} \in \text{cog}(L/\mathcal{K})$ tal que $\beta^{P^2} = b \in \mathcal{K}$. Entonces, como $L/K(\lambda_P)$ es radical, se sigue de la Proposición 10.5.3 que $\lambda_{P^2} \in L$. Consideremos el siguiente diagrama

$$\begin{array}{ccc}
\mathcal{O}_L & \text{-----} & L \\
| & & | \\
\mathcal{O}_{K(\lambda_{P^2})} & \text{-----} & K(\lambda_{P^2}) \\
| & & | \\
\mathcal{O}_{K(\lambda_P)} & \text{-----} & K(\lambda_P) \\
| & & | \\
R_T & \text{-----} & K
\end{array}$$

El índice de ramificación del primo P en la extensión $K(\lambda_{P^2})/K$, es $\Phi(P^2)$ por lo que el índice de ramificación de P en la extensión L/K es $d\Phi(P^2)$, donde $\tilde{d} = e_{L/\mathcal{K}(\lambda_{P^2})}$. Del Teorema 3.9. de [66] tenemos que el índice de ramificación es $\Phi(P)$. En otras palabras, $d\Phi(P^2) = \Phi(P)$, lo cual es absurdo, de donde se sigue la afirmación. \square

Ejemplo 10.8.11. Sean $P, Q \in R_T$, irreducibles y distintos. Considere la extensión $L = K(\Lambda_{P^2Q^2})/K$. Notemos que $L = K(\lambda_{P^2}, \lambda_{Q^2})$. Sea $\sigma = 1 + PQ \in G = \text{Gal}(L/K)$. Se tiene que $\sigma \neq 1$ ya que $\lambda_{P^2Q^2}^{1+PQ} = \lambda_{P^2Q^2} + \lambda_{PQ} \neq \lambda_{P^2Q^2}$.

Se tiene que $\sigma(\lambda_{PQ}) = \lambda_{PQ}^{1+PQ} = \lambda_{PQ}$. Por lo tanto si \mathcal{K} es el campo fijo de (σ) , se tiene que $\lambda_{PQ} \in \mathcal{K}$.

Por otro lado se tiene que $\sigma^p = (1 + PQ)^p = 1 + P^pQ^p \equiv 1 \pmod{P^2Q^2}$, es decir, el orden de σ es p . Por lo tanto $[L : \mathcal{K}] = p$.

Puesto que $\sigma(\lambda_{P^2}) = \lambda_{P^2} + \lambda_P^Q \neq \lambda_{P^2}$, se tiene que $\lambda_{P^2} \notin \mathcal{K}$. De modo análogo se puede mostrar que $\beta = \lambda_{Q^2} \notin \mathcal{K}$.

Ahora, como $[L : \mathcal{K}] = p$, se tiene que $L = \mathcal{K}(\alpha) = \mathcal{K}(\beta)$, además $\alpha^P = \lambda_P$ y $\beta^Q = \lambda_Q$. Por lo tanto el módulo $\text{cog}(L/\mathcal{K})$, tiene elementos de orden P y de orden Q .

Ejemplo 10.8.12. Sea $q = p^\nu$ con $p \geq 3$. Sea $L = K(\Lambda_{P^3})$ y $\sigma = 1 + P \in \text{Gal}(L/K(\Lambda_P))$. Se tiene que $\sigma^p = (1 + P)^p \equiv 1 \pmod{P^3}$. Además $\sigma \neq 1$ ya que $\sigma(\lambda_{P^3}) = \lambda_{P^3} + \lambda_{P^2} \neq \lambda_{P^3}$.

Sea $\mathcal{K} = L^{(\sigma)}$, se tiene que $[L : \mathcal{K}] = p$. Por otra parte $\sigma(\lambda_{P^2}) = \lambda_{P^2} + \lambda_P \neq \lambda_{P^2}$. Por lo tanto $\alpha = \lambda_{P^2} \notin \mathcal{K}$. Así $L = \mathcal{K}(\alpha)$ y $\alpha^P = a \in \mathcal{K}$.

Ahora bien, $\lambda_{P^3} \in L$ tiene orden P^2 ya que $\lambda_{P^3}^{P^2} \in \mathcal{K}$ y $\lambda_{P^3}^P \notin \mathcal{K}$. Por lo tanto el módulo $\text{cog}(L/\mathcal{K})$ tiene elementos de orden P^2 .

Los Ejemplos 10.8.11 y 10.8.12 muestran que no tenemos los análogos del Lema 1.3. de [18], a saber si L/\mathcal{K} es cogalois, en el sentido clásico, y es tal que $[L : \mathcal{K}] = p$, con $L = \mathcal{K}(\alpha)$ con $\alpha^p = a \in \mathcal{K}$ y L/\mathcal{K} es separable y pura, entonces

- (a) El grupo $\operatorname{cog}(L/\mathcal{K})$ no tiene elementos de orden $q \neq p$, q un número primo.
- (b) El grupo $\operatorname{cog}(L/\mathcal{K})$ no tiene elementos de orden p^2 .

10.9. Una cota para $|\operatorname{cog}(L/\mathcal{K})|$

En esta sección establecemos una cota superior para la cardinalidad del módulo $\operatorname{cog}(L/\mathcal{K})$. En lo que sigue sea $q = p^\nu$ y sea L/\mathcal{K} una extensión radical.

Lema 10.9.1. *Sea \mathcal{K}/K una extensión finita. Entonces $\mu(\mathcal{K}) = \Lambda_M$ para algún $M \in R_T$.*

Demostración. Se tiene $\mu(\mathcal{K}) = \{u \in \mathcal{K} \mid \text{existe } M \in R_T \text{ tal que } u^M = 0\}$. Entonces $\mu(\mathcal{K})$ es un R_T -módulo pues si $z \in \mu(\mathcal{K})$, consideremos $N \in R_T$ tal que $z^N = 0$. Sea $N' \in R_T$ arbitrario. Se tiene $(z^{N'})^N = z^{N'N} = z^{NN'} = (z^N)^{N'} = 0^{N'} = 0$.

Sea $P \in R_T$ un polinomio mónico e irreducible y sea $\mu(\mathcal{K})(P) = \{u \in \mathcal{K} \mid \text{exite } n \in \mathbb{N} \text{ tal que } u^{P^n} = 0\}$ la P -torsión de $\mu(\mathcal{K})$. Entonces $\mu(\mathcal{K})(P)$ es un R_T -submódulo de $\mu(\mathcal{K})$ y se tiene

$$\mu(\mathcal{K}) = \bigoplus_{\substack{P \in R_T \\ P \text{ mónico e irreducible}}} \mu(\mathcal{K})(P).$$

Fijemos $P \in R_T$ mónico e irreducible tal que $\mu(\mathcal{K})(P) \neq 0$ y consideremos $n \in \mathbb{N}$ el mínimo tal que $u^{P^n} = 0$ para todo $u \in \mu(\mathcal{K})(P)$, esto es, existe $z \in \mu(\mathcal{K})(P)$ tal que $z^{P^{n-1}} \neq 0$. Sea $u \in \mu(\mathcal{K})(P)$. Entonces $u^{P^s} = 0$ con $s \leq n$. Por tanto $u^{P^n} = (u^{P^s})^{P^{n-s}} = 0^{P^{n-s}} = 0$. Se sigue que $\mu(\mathcal{K})(P) \subseteq \Lambda_{P^n}$.

Por otro lado, existe $\lambda \in \mu(\mathcal{K})(P)$ con $\lambda^{P^n} = 0$ y $\lambda^{P^{n-1}} \neq 0$. En particular $\lambda \in \Lambda_{P^n} \setminus \Lambda_{P^{n-1}}$ por lo que λ es un generador de Λ_{P^n} y se tiene que por ser $\mu(\mathcal{K})(P)$ es un R_T -módulo $\{\lambda^A\}_{A \in R_T} = \Lambda_{P^n} \subseteq \mu(\mathcal{K})(P)$. Se sigue que $\mu(\mathcal{K})(P) = \Lambda_{P^n}$.

Por tanto

$$\begin{aligned} \mu(\mathcal{K}) &= \bigoplus_{\substack{P \in R_T \\ P \text{ mónico e irreducible}}} \mu(\mathcal{K})(P) = \bigoplus_{\substack{P \in R_T \\ P \text{ mónico e irreducible} \\ \mu(\mathcal{K})(P) \neq 0}} \mu(\mathcal{K})(P) \\ &= \bigoplus_{j=1}^r \Lambda_{P_j^{\alpha_j}} = \Lambda_{P_1^{\alpha_1} \dots P_r^{\alpha_r}} = \Lambda_M \end{aligned}$$

donde $M = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. □

Observación 10.9.2. Si la extensión L/\mathcal{K} es de Galois y radical ciclotómica y tal que $\mu(\mathcal{K}) = \mu(L)$, entonces al ser radical L es de la forma $\mathcal{K}(\rho_1, \dots, \rho_t)$, con $\rho^{M_i} = a_i \in \mathcal{K}$, para algunos $M_i \in R_T$. Por otra parte las raíces de $X^{M_i} - a_i$ son $\{\rho_i + \lambda_{M_i}^A\}_{A \in R_T}$. Por lo tanto $\text{Gal}(\mathcal{K}(\rho_i)/\mathcal{K}) \subseteq \Lambda_{M_i}$. De esta manera $\text{Gal}(\mathcal{K}(\rho_i)/\mathcal{K})$ es un p -grupo elemental abeliano.

Puesto que se tiene una inyección

$$\text{Gal}(L/\mathcal{K}) \hookrightarrow \prod_{i=1}^t \text{Gal}(\mathcal{K}(\rho_i)/\mathcal{K})$$

se sigue que $\text{Gal}(L/\mathcal{K})$ es un p -grupo elemental abeliano.

Si L/K es una extensión finita y $\mu(L) = \Lambda_M$, definimos

$$\text{gr}(\mu(L)) = \text{gr}(M).$$

Lema 10.9.3. Sea L/\mathcal{K} una extensión finita de Galois radical ciclotómica. Entonces existe un isomorfismo

$$B^1(G, \mu(L)) \cong \mu(L)/\mu(\mathcal{K})$$

como R_T -módulos.

Demostración. Se define $\psi: \mu(L) \rightarrow B^1(G, \mu(L))$ como sigue: $\psi(u) = f_u$. Observemos que $\psi(u+v) = \psi(u) + \psi(v)$ ya que

$$\begin{aligned} (f_u + f_v)(\sigma) &= f_u(\sigma) + f_v(\sigma) = \sigma(u) - u + \sigma(v) - v \\ &= \sigma(u+v) - (u+v) = (f_{u+v})(\sigma). \end{aligned}$$

y si $M \in R_T$ se tendrá que $\psi(u^M) = f_{u^M} = f_u^M$, ya que

$$\begin{aligned} f_{u^M}(\sigma) &= \sigma(u^M) - u^M = (\sigma(u))^M - u^M \\ &= (\sigma(u) - u)^M = (f_u(\sigma))^M. \end{aligned}$$

Por tanto ψ es un homomorfismo de R_T -módulos, suprayectivo por la definición de $B^1(G, \mu(L))$. Puesto que L/\mathcal{K} es una extensión de Galois tenemos $\text{nuc}(\psi) = \mu(\mathcal{K})$. \square

Proposición 10.9.4. Sea L/\mathcal{K} una extensión Galois y radical ciclotómica. Supongamos que $\mu(L) = \mu(\mathcal{K})$. Entonces

$$|\text{cog}(L/\mathcal{K})| = q^{m \text{gr}(\mu(L))},$$

donde $[L : \mathcal{K}] = p^m$.

Demostración. Por la Observación 10.9.2 se tiene que $\text{Gal}(L/\mathcal{K}) \cong C_p^m$, para algún $m \in \mathbb{N}$. Puesto que $B^1(G, \mu(L)) = \{0\}$ y $H^1(G, \mu(L)) \cong \text{Hom}(G, \mu(L))$, entonces de la Proposición 10.6.4, se tiene que

$$\operatorname{cog}(L/\mathcal{K}) \cong Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong H^1(G, \mu(L)) \cong \operatorname{Hom}(G, \mu(L)).$$

Además $\mu(L) \cong C_p^{\nu \operatorname{gr}(\mu(L))}$. Por tanto, si denotamos por $\mathfrak{L}_p(\mathbb{F}_p^m, \mathbb{F}_p^{\nu \operatorname{gr}(\mu(L))})$ al conjunto de las transformaciones lineales de \mathbb{F}_p^m a $\mathbb{F}_p^{\nu \operatorname{gr}(\mu(L))}$ y al conjunto de las matrices $m \times \nu \operatorname{gr}(\mu(L))$ con coeficientes en \mathbb{F}_p lo denotamos por $\mathfrak{M}_{m \times \nu \operatorname{gr}(\mu(L))}(\mathbb{F}_p)$, se tiene

$$\begin{aligned} \operatorname{Hom}(G, \mu(L)) &= \operatorname{Hom}(C_p^m, C_p^{s \operatorname{gr}(\mu(L))}) = \mathfrak{L}_p(\mathbb{F}_p^m, \mathbb{F}_p^{s \operatorname{gr}(\mu(L))}) \\ &= \mathfrak{M}_{m \times s \operatorname{gr}(\mu(L))}(\mathbb{F}_p). \end{aligned}$$

Por tanto $|\operatorname{Hom}(G, \mu(L))| = q^{m \operatorname{gr}(\mu(L))}$. \square

Ejemplo 10.9.5. Del Ejemplo 10.8.7, se sigue que la extensión $L/K(\Lambda_T)$, donde L es el campo de descomposición del polinomio $f(X) = X^T - 1$, cumple que $|\operatorname{cog}(L/K(\Lambda_T))| = [L : K(\Lambda_T)] = q = q^{m \operatorname{gr}(\mu(L))}$, en concordancia con la Proposición 10.9.4.

Proposición 10.9.6. Sea L/\mathcal{K} una extensión Galois y radical ciclotómica y supongamos que $L = \mathcal{K}(\mu(L))$. Entonces $|\operatorname{cog}(L/\mathcal{K})| \leq q^{m \operatorname{gr}(\mu(L))}$ para alguna $m \in \mathbb{N}$.

Demostración. Por el Corolario 10.7.9 se tiene que $[L : \mathcal{K}] = p^m$ para alguna $m \in \mathbb{N}$. Ahora la demostración es por inducción sobre m . Sea L/\mathcal{K} una extensión Galois, radical ciclotómica, tal que $L = \mathcal{K}(\mu(L))$ y $[L : \mathcal{K}] = p$. Por lo tanto L/\mathcal{K} es cíclica de grado p . Sean $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ y $N = P_1^{\beta_1} \cdots P_r^{\beta_r}$, con $1 \leq \beta_i \leq \alpha_i$, donde $i = 1, \dots, r$, tales que $\mu(L) = \Lambda_M$ y $\mu(\mathcal{K}) = \Lambda_N$.

Sea $G := \operatorname{Gal}(L/\mathcal{K}) = \langle \sigma \rangle$. Se tiene $\sigma(\lambda_M) = \lambda_M^A$ ya que la acción de Carlitz-Hayes conmuta con σ . Notemos que $\sigma(\lambda_M) \neq \lambda_M$, en caso contrario esto implicaría que $\lambda_M \in \mathcal{K}$, es decir, $L = \mathcal{K}$ lo cual es una contradicción. Por lo tanto $M \nmid (A-1)$. Sea $M = ND$. Por lo tanto $\lambda_N = \lambda_N^D$. Se tiene que

$$\lambda_N = \sigma(\lambda_N) = \sigma(\lambda_M^D) = (\sigma(\lambda_M))^D = \lambda_M^{AD} = \lambda_N^A.$$

Se sigue que $\lambda_N^{A-1} = 0$, es decir, $N \mid (A-1)$.

Por otro lado

$$\begin{aligned} \operatorname{Tr}_G(\lambda_M) &= \lambda_M + \lambda_M^A + \lambda_M^{A^2} + \cdots + \lambda_M^{A^{p-1}} \\ &= \lambda_M^{1+A+A^2+\cdots+A^{p-1}} = \lambda_M^{\frac{A^p-1}{A-1}} = \lambda_M^{(A-1)^{p-1}} \end{aligned}$$

donde la última igualdad se debe a que $\frac{A^p-1}{A-1} = \frac{(A-1)^p}{A-1}$.

Por lo tanto $\operatorname{Tr}_G(\lambda_M) \in \mathcal{K} \cap \Lambda_M = \Lambda_N$. De aquí se obtiene que existe $C \in R_T$ tal que $\lambda_M^{(A-1)^{p-1}} = \lambda_N^C$. Como $\sigma^p = 1$ se tiene que $\sigma^p(\lambda_M) = \lambda_M^A = \lambda_M$, es decir, $\lambda_M^{A^p-1} = 0$. Puesto que $A^p - 1 = (A-1)^p$, tenemos que $M \mid (A-1)^p$.

Podemos escribir $A - 1 = P_1^{\gamma_1} \cdots P_r^{\gamma_r} Q$ con $(Q, P_1 \cdots P_r) = 1$. Ahora si $\beta_i < \alpha_i$ se tiene que $\lambda_{NP_i} \in L \setminus \mathcal{K}$ por lo tanto $\sigma(\lambda_{NP_i}) = \lambda_{NP_i}^A \neq \lambda_{NP_i}$. Por lo tanto $NP_i \nmid (A - 1)$.

De aquí se sigue lo siguiente:

- (i) Puesto que $M \nmid (A - 1)$ se tiene que $\gamma_{i_0} < \alpha_{i_0}$ para algún $i_0 \in \{1, \dots, r\}$.
- (ii) Puesto que $N \mid (A - 1)$ se tiene que $\beta_i \leq \gamma_i$. Ya que $NP_i \nmid (A - 1)$, entonces $\beta_i + 1 > \gamma_i$. Se sigue que $\beta_i = \gamma_i$.

(iii) Como $\lambda_M^{(A-1)^{p-1}} = \lambda_N^C$ se tiene que $\alpha_i - (p-1)\gamma_i \leq \beta_i$, para $1 \leq i \leq r$.

(iv) De $M \mid (A - 1)^p$ se sigue que $\alpha_i \leq p\gamma_i$, para $1 \leq i \leq r$.

Ahora $\text{Tr}_G(\lambda_M^B) = (\text{Tr}(\lambda_M))^B = \lambda_M^{B(A-1)^{p-1}}$ para cualquier $B \in R_T$.

Sea $B = P_1^{\delta_1} \cdots P_r^{\delta_r} R$ con $(R, P_1 \cdots P_r) = 1$. Se tiene

$$\begin{aligned} \lambda_M^B \in \text{nuc Tr}_G &\Leftrightarrow \delta_i + (p-1)\gamma_i \geq \alpha_i \text{ para cada } i \\ &\Leftrightarrow \delta_i \geq 0 \text{ y } \delta_i + (p-1)\gamma_i \geq \alpha_i \text{ para cada } i \\ &\Leftrightarrow \delta_i \geq \max\{0, \alpha_i - (p-1)\gamma_i\} \text{ para cada } i. \end{aligned}$$

Por lo tanto $\text{nuc Tr}_G = (\lambda_M^B)$ con $B = P_1^{\delta_1} \cdots P_r^{\delta_r}$ y $\delta_i = \max\{0, \alpha_i - (p-1)\gamma_i\}$ con $1 \leq i \leq r$. Así $(\lambda_M^B) = (\lambda_{M'})$, con $M' = P_1^{\mu_1} \cdots P_r^{\mu_r}$ donde $\mu_i = \alpha_i - \delta_i$, $1 \leq i \leq r$.

Además $I_G(\lambda_M) = ((\sigma - 1)\lambda_M) = (\lambda_M^{A-1})$, donde $I_G : \mu(L) \rightarrow \mu(L)$ es el homomorfismo definido por $I_G(u) = \sigma(u) - u$. Por otro lado $I_G(\lambda_M) = (\lambda_{M''})$, con $M'' = P_1^{\varphi_1} \cdots P_r^{\varphi_r}$, donde $\varphi_i = \max\{\alpha_i - \gamma_i, 0\}$, $1 \leq i \leq r$.

De (ii) obtenemos que $\varphi_i = \alpha_i - \beta_i$ si $\beta_i < \alpha_i$. Si $\alpha_i = \beta_i$ de (ii) se obtiene que $\alpha_i - \gamma_i \leq 0$. Por lo tanto $\varphi_i = \alpha_i - \beta_i$.

Así, se tiene que

$$|H^1(G, \mu(L))| = \frac{|\lambda_{M'}|}{|\lambda_{M''}|} = |\lambda_{M'''}|$$

con $M''' = P_1^{\varepsilon_1} \cdots P_r^{\varepsilon_r}$ donde

$$\varepsilon_i = \mu_i - \varphi_i = \alpha_i - \delta_i - (\alpha_i - \beta_i) = \beta_i - \delta_i, \quad 1 \leq i \leq r.$$

Obviamente $\varepsilon_i \leq \beta_i$, por tanto

$$|H^1(G, \mu(L))| = q^{\text{gr } M'''} \leq q^{\text{gr } N}.$$

Combinando esta desigualdad y el Lema 10.9.3, obtenemos

$$\begin{aligned} |\text{cog}(L/\mathcal{K})| &= |H^1(G, \mu(L))| |B^1(G, \mu(L))| = |H^1(G, \mu(L))| \frac{|\mu(L)|}{|\mu(\mathcal{K})|} \\ &= q^{\text{gr } M'''} q^{\text{gr } M - \text{gr } N} \leq q^{\text{gr } M} = q^{\text{gr}(\mu(L))}. \end{aligned}$$

Ahora sea $[L : \mathcal{K}] = p^m$ para algún $m \in \mathbb{N}$, $m \geq 2$. Sea H un subgrupo de G de orden p^{m-1} . Sea $E = L^H$. Entonces $\mathcal{K} \subseteq E \subseteq L$. Tenemos $[E : \mathcal{K}] = p$, $[L : E] = p^{m-1}$ y $L = E(\mu(L))$.

Si E/\mathcal{K} no fuera radical ciclotómica, entonces $\operatorname{cog}(E/\mathcal{K}) = \{0\}$, ya que en caso contrario existe $\bar{\alpha} \in \operatorname{cog}(E/\mathcal{K})$ no cero. En particular $\alpha \notin \mathcal{K}$. De esta manera $E = \mathcal{K}(\alpha)$, pero esto implica que E/\mathcal{K} es radical ciclotómica, lo cual es absurdo.

Si E/\mathcal{K} es radical ciclotómica se tienen dos casos a considerar

- (i) $\mu(E) \neq \mu(\mathcal{K})$ y
- (ii) $\mu(E) = \mu(\mathcal{K})$.

En el caso (i), por lo demostrado para el caso $[E : \mathcal{K}] = p$ se tiene que

$$|\operatorname{cog}(E/\mathcal{K})| \leq q^{\operatorname{gr}(\mu(E))}.$$

En el caso (ii), por la Proposición 10.9.4 se tiene que $|\operatorname{cog}(E/\mathcal{K})| = q^{\operatorname{gr}(\mu(E))}$. Así, en cualquier caso,

$$|\operatorname{cog}(E/\mathcal{K})| \leq q^{\operatorname{gr}(\mu(E))} \leq q^{\operatorname{gr}(\mu(L))}.$$

Por lo tanto, puesto que $L = E(\mu(L))$ y $[L : E] = p^{m-1}$, por inducción se tiene que $|\operatorname{cog}(L/E)| \leq q^{(m-1)\operatorname{gr}(\mu(L))}$. Por lo tanto de la sucesión exacta

$$0 \rightarrow \operatorname{cog}(E/\mathcal{K}) \rightarrow \operatorname{cog}(L/\mathcal{K}) \rightarrow \operatorname{cog}(L/E)$$

se tiene que $|\operatorname{cog}(L/\mathcal{K})| \leq |\operatorname{cog}(E/\mathcal{K})| |\operatorname{cog}(L/E)| \leq q^{m\operatorname{gr}(\mu(L))}$. \square

De la demostración de la Proposición 10.9.6, para el caso $m = 1$, se tiene el siguiente teorema.

Teorema 10.9.7. *Sea L/\mathcal{K} cíclica de grado p , $L = \mathcal{K}(\alpha)$ tal que $\alpha \in \operatorname{cog}(L/\mathcal{K})$. Entonces L/\mathcal{K} es radical ciclotómica, $|\operatorname{cog}(L/\mathcal{K})| = p^{\nu t}$, donde $q = p^{\nu}$ y*

$$t = \begin{cases} \operatorname{gr}(\mu(L)) - \operatorname{gr}(\mu(\mathcal{K})) + \operatorname{gr}(\frac{B-1}{C}) & \text{si } \mu(L) \neq \mu(\mathcal{K}), \\ \operatorname{gr}(\mu(L)) & \text{si } \mu(L) = \mu(\mathcal{K}). \end{cases}$$

donde $\sigma(\lambda_M) = \lambda_M^B$, $B-1 = \operatorname{mcd}(A-1, B)$ y C es de grado mínimo tal que $C \mid (B-1)$ y $M \mid C(B-1)^{p-1}$. \square

Proposición 10.9.8. *Sea L/\mathcal{K} una extensión Galois radical ciclotómica. Entonces*

$$|\operatorname{cog}(L/\mathcal{K})| \leq q^{m\operatorname{gr}(\mu(L))}.$$

donde $[L : \mathcal{K}] = p^m$.

Demostración. Sea $E = \mathcal{K}(\mu(L))$ con $\mathcal{K} \subseteq E \subseteq L$, entonces

$$|\operatorname{cog}(L/\mathcal{K})| \leq |\operatorname{cog}(E/\mathcal{K})| |\operatorname{cog}(L/E)| \leq q^{m\operatorname{gr}(\mu(L))}$$

por la Proposiciones 10.9.4 y 10.9.6. \square

El ejemplo siguiente muestra que la desigualdad de la Proposición 10.9.8 puede ser estricta.

Ejemplo 10.9.9. Sea $L = K(\Lambda_{P^{2p-1}})$, con $P \in R_T$ irreducible, y $\sigma = 1 + P^2 \in \text{Gal}(K(\Lambda_{P^{2p-1}})/K)$. Se tiene

$$\sigma(\lambda_{2p-1}) = \lambda_{P^{2p-1}} + \lambda_{P^{2p-3}} \neq \lambda_{P^{2p-1}}$$

de este modo $\sigma \neq 1$.

Por otro lado se tiene que $\sigma^p = (1 + P^2)^p = 1 + P^{2p}$, de esta manera

$$\sigma^p(\lambda_{P^{2p-1}}) = \lambda_{P^{2p-1}} + \lambda_{P^{2p-1}}^{P^{2p}} = \lambda_{P^{2p-1}}.$$

Por lo tanto $\sigma^p = 1$, así el orden de σ es p .

Sea $E = L^{(\sigma)}$. Entonces $[L : E] = p$ y L/E es radical ciclotómica. Se tiene que $\sigma(\lambda_{P^{2p-1}}^M) = \lambda_{P^{2p-1}}^M + \lambda_{P^{2p-3}}^M = \lambda_{P^{2p-1}}^M$ si y sólo si el exponente en que aparece P en la descomposición de M es mayor o igual a $2p-3$. En este caso $\lambda_{P^{2p-1}}^{P^{2p-3}} = \lambda_{P^2} \in E$. Notemos que $\lambda_{P^3} \notin E$. Por lo tanto $\mu(E) = \Lambda_{P^2}$. Además $\mu(L) = \Lambda_{P^{2p-1}}$.

Ahora sea $N_{\mu(L)}$ el mapeo traza de L a E , esto es, $N_{\mu(L)} = \sum_{i=0}^{p-1} \sigma^i$.

Tenemos $N_{\mu(L)}(\lambda_{P^{2p-1}}^M) = \lambda_{P^{2p-1}}^{M(\frac{(1+P^2)^{p-1}}{(1+P^2)-1})} = \lambda_{P^{2p-1}}^{MP^{2p-2}} = \lambda_P^M = 0$ si y sólo si P divide a M . Por lo tanto nú $N_{\mu(L)} = (\lambda_{P^{2p-1}}^P) = \Lambda_{P^{2p-2}}$.

Sea $G := \text{Gal}(L/E) = \langle \sigma \rangle$ y $I_G := \langle \sigma - 1 \rangle$. Entonces $I_G(\mu(L)) = (\sigma(\lambda_{P^{2p-1}}) - \lambda_{P^{2p-1}}) = (\lambda_{P^{2p-3}}) = \Lambda_{P^{2p-3}}$. Por lo tanto

$$|\text{cog}(L/E)| = |H^1(G, \mu(L))| = \frac{|\mu(L)|}{|\mu(E)|} = \frac{|\Lambda_{P^{2p-2}}|}{|\Lambda_{P^{2p-3}}|} \frac{|\Lambda_{P^{2p-1}}|}{|\Lambda_{P^2}|} = q^{d(2p-2)}$$

donde $d = \text{gr}(P)$. Puesto que $m = 1$, se tiene

$$|\text{cog}(L/E)| = q^{d(2p-2)} < q^{d(2p-1)} = q^{m \text{gr}(\mu(L))}.$$

Teorema 10.9.10. Sea L/\mathcal{K} una extensión radical ciclotómica. Entonces si \tilde{L} es la cerradura de Galois de L , se tendrá

$$|\text{cog}(L/\mathcal{K})| \leq q^{m \text{gr}(\mu(\tilde{L}))}$$

donde $[\tilde{L} : \mathcal{K}] = p^m$.

Demostración. Sea $G = \text{Gal}(\tilde{L}/\mathcal{K}) = HN$ con H un subgrupo normal de G , N el p subgrupo de Sylow. Sea $F = \tilde{L}^H$. Se puede suponer que $F = L$ cambiando H por un conjugado. De aquí tenemos el diagrama

$$\begin{array}{ccc} L & \xrightarrow{H} & \tilde{L} \\ \downarrow & & \downarrow N \\ \mathcal{K} & \xrightarrow{\quad} & E \end{array}$$

Sea $\alpha \in \text{cog}(L/\mathcal{K})$, distinto de cero, así existe un $N \in R_T$ tal que $\alpha^N = a \in \mathcal{K}$. Puesto que $\alpha \in \tilde{L}$, $\alpha^N \in \mathcal{K} \subseteq E$, es decir, $\alpha \in \text{cog}(\tilde{L}/E)$. Si $\alpha = 0$

en $\operatorname{cog}(\tilde{L}/E)$ tendríamos $\alpha \in E \cap L = \mathcal{K}$ por lo que $\alpha = 0$ en $\operatorname{cog}(L/\mathcal{K})$ lo cual es una contradicción.

Por lo tanto $\operatorname{cog}(L/\mathcal{K}) \subseteq \operatorname{cog}(\tilde{L}/E)$.

De esta manera $|\operatorname{cog}(L/\mathcal{K})| \leq |\operatorname{cog}(\tilde{L}/E)| \leq q^{m \operatorname{gr}(\mu(\tilde{L}))}$. \square

Extensiones p -cíclicas en característica p

11.1. Introducción

Recordemos la definición de extensiones de Kummer (ver Definición 10.1.3).

Definición 11.1.1. Una *extensión de Kummer* finita es una extensión de Galois L/K donde el grupo de Galois de la extensión es $G = \text{Gal}(L/K)$ un grupo cíclico finito C_n de orden n y tal que K contiene al conjunto $\mu_n = \langle \zeta_n \rangle$ de las n -raíces de unidad y donde la característica de K no divide a n .

Las extensiones de Kummer están caracterizadas por

$$\langle \zeta_n \rangle \subseteq K, \quad L = K(\sqrt[n]{\alpha}), \quad \alpha \in L \quad \text{y} \quad f(x) := \text{Irr}(\alpha, x, K) = x^n - \alpha^n.$$

Las raíces de $f(x)$ son $\{\zeta_n^i \alpha\}_{i=0}^{n-1}$. En el caso de que la característica p de K divide a n , el grupo de las p -raíces de la unidad es el grupo trivial $\mu_p = \{1\}$ ya que en característica p tenemos que $\xi^p = 1 = 1^p$ lo cual implica que $(\xi^p - 1^p) = (\xi - 1)^p = 0$ por lo que $\xi = 1$.

Los primeros en considerar las extensiones cíclicas de grado p en característica p fueron E. Artin y O. Schreier [3]. Ellos probaron que una ecuación $x^p - x - a$ o bien proporciona una extensión cíclica de grado p o bien todas sus raíces están en el campo base pues si α es una raíz cualquiera de $x^p - x - a$ entonces $\{\alpha, \alpha + 1, \dots, \alpha + (p-1)\}$ son todas las raíces del polinomio. Artin y Schreier probaron el recíproco, esto es, toda extensión cíclica de grado p en característica p está generada por un polinomio irreducible de la forma $f(x) = x^p - x - a \in K[x]$. En ese mismo trabajo, Artin y Schreier estudiaron extensiones cíclicas de grado p^2 .

Usando las técnicas de Artin-Schreier, A. Albert [1] encontró una descripción recursiva de generación de todas las extensiones cíclicas de grado p^n en característica p y probó que cualquier extensión cíclica de grado p es una subextensión de una extensión cíclica de grado p^n . En particular, si podemos generar una extensión cíclica de grado p en característica p , entonces existen extensiones cíclicas de grado p^n para toda $n \in \mathbb{N}$.

En [77], E. Witt encontró condiciones necesarias y suficientes para que un elemento $\theta \in K$, sea tal que $K = k(\theta)$ sea una extensión cíclica de grado p^f , $f \geq 2$, sobre k que contiene a una extensión cíclica R/k dada de grado p^{f-1} . Usando este resultado, H.L. Schmid [64] dio una caracterización de todas las extensiones cíclicas de grado p^n , K/k , por medio de elementos $\beta_1, \beta_2, \dots, \beta_n \in k$. Schmid dio, de manera recursiva, las ecuaciones que generan estas extensiones. E. Witt [78] encontró una forma vectorial de describir las extensiones cíclicas de grado p^n halladas por Schmid. Esta forma vectorial es lo que conocemos como *vectores de Witt*.

Inmediatamente después de los resultados de Witt, Schmid [65] interpretó los resultados aritméticos que había obtenido anteriormente en [64] y los puso en términos de los vectores de Witt.

El principal objetivo de este capítulo es presentar la teoría elemental de los vectores de Witt como generadores de extensiones cíclicas de grado p^n y la aritmética de estos campos obtenida por Schmid. En particular daremos una breve introducción del concepto de *conductor* de un campo.

En este capítulo todos los campos considerados serán de característica p .

11.2. Extensiones de Artin–Schreier

Empezamos por recordar la teoría de las extensiones cíclicas de grado p .

Teorema 11.2.1 (E. Artin y O. Schreier [3]). *Sea $f(x) = x^p - x - a \in k[x]$ un polinomio irreducible. Sea $K = k(\alpha)$, donde α es una raíz de $f(x)$. Entonces K/k es una extensión cíclica de grado p .*

Recíprocamente, si K/k es una extensión cíclica de grado p , existe $\alpha \in K$ tal que $\text{Irr}(\alpha, x, k) = x^p - x - a$ para algún $a \in k$.

Demostración. Sea $\alpha \in \bar{k}$, \bar{k} una cerradura algebraica de k , cualquier raíz de $f(x)$. Entonces las raíces de $f(x)$ son $\{\alpha + i\}_{i=0}^{p-1}$. En particular K/k es una extensión normal y separable y existe $\sigma \in G := \text{Gal}(K/k)$ con $\sigma\alpha = \alpha + 1$. Entonces $o(\sigma) = p$ y $G = \langle \sigma \rangle$ es cíclico de orden p .

Recíprocamente, sea K/k una extensión cíclica de grado p , digamos $K = k(\beta)$. Sea σ un generador de $G = \text{Gal}(K/k)$, $o(\sigma) = p$. Sean $\sigma^i\beta = \beta_i$, $i = 0, \dots, p-1$, los conjugados de β . Se tiene $\sigma\beta_i = \beta_{i+1}$, $i = 0, \dots, p-1$. Notemos que $\beta_0 = \beta_p = \beta$. Consideremos el determinante de Vandermonde:

$$\det(\beta_i^j)_{0 \leq i, j \leq p-1} = \prod_{i < j} (\beta_i - \beta_j) \neq 0.$$

En particular, la matriz $(\beta_i^j)_{0 \leq i, j \leq p-1}$ es no singular y existe $0 \leq j \leq p-1$ tal que $\gamma := \sum_{i=0}^{p-1} \beta_i^j \neq 0$. Sea $\alpha := -\frac{1}{\gamma} \sum_{i=0}^{p-1} i\beta_i^j$. Se tiene

$$\begin{aligned}
\sigma\alpha &= -\frac{1}{\sigma\gamma} \sum_{i=0}^{p-1} i\sigma(\beta_i^j) = -\frac{1}{\gamma} \sum_{i=0}^{p-1} i(\beta_{i+1}^j) = -\frac{1}{\gamma} \left(\sum_{i=0}^{p-1} (i+1)\beta_{i+1}^j - \sum_{i=0}^{p-1} \beta_i^j \right) \\
&= -\frac{1}{\gamma} \sum_{i=1}^p i\beta_i^j + \frac{1}{\gamma} \sum_{i=0}^{p-1} \beta_i^j = -\frac{1}{\gamma} \sum_{i=0}^{p-1} i\beta_i + 1 = \alpha + 1.
\end{aligned}$$

Entonces $\{\sigma^i\alpha\}_{i=0}^{p-1} = \{\alpha + i\}_{i=0}^{p-1}$ son conjugados. Notemos que

$$\sigma(\alpha^p - \alpha) = (\sigma\alpha)^p - (\sigma\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha,$$

de donde se sigue que $\alpha^p - \alpha \in k$. De esta forma obtenemos que $\text{Irr}(\alpha, x, k) = x^p - x - a$ donde $a := \alpha^p - \alpha$. \square

Corolario 11.2.2. Si K/k es una extensión cíclica de grado p con $K = k(\alpha) = k(\beta)$ y $\text{Irr}(\alpha, x, k) = x^p - x - a$, $\text{Irr}(\beta, x, k) = x^p - x - b$, entonces existen $j \in \{1, 2, \dots, p-1\}$ y $c \in k$ tales $\alpha = j\beta + c$ y $a = jb + c^p - c$ y recíprocamente.

Demostración. Sea $\sigma \in \text{Gal}(K/k)$ tal que $\sigma\alpha = \alpha + 1$. Puesto que $\sigma\beta$ es conjugado a β , existe $i \in \{1, 2, \dots, p-1\}$ tal que $\sigma\beta = \beta + i$. Sea $j \in \{1, 2, \dots, p-1\}$ tal que $ji \equiv 1 \pmod{p}$. Entonces

$$\sigma(\alpha - j\beta) = \sigma\alpha - j\sigma\beta = (\alpha + 1) - j(\beta + i) = \alpha - j\beta + 1 - ji = \alpha - j\beta,$$

de donde se sigue que $\alpha - j\beta \in k$. Ahora

$$\begin{aligned}
a &= \alpha^p - \alpha = (j\beta + c)^p - (j\beta + c) = j^p\beta^p + c^p - j\beta - c \\
&= j\beta^p - j\beta + c^p - c = j(\beta^p - \beta) + (c^p - c) = jb + c^p - c.
\end{aligned}$$

El recíproco es similar. \square

Notación 11.2.3. Sea $a \in k$, un campo de característica p . Se denota $\wp(a) := a^p - a$.

Como mencionamos en la introducción, Artin y Schreier profundizaron su método y encontraron las extensiones cíclicas de grado p^2 . Su técnica fue el primer paso para lo que vendría en los siguientes años: los resultados de Albert, Schmid y Witt.

Veamos como podemos construir extensiones cíclicas de grado p^n en característica p . Sea G un grupo cíclico de orden p^n . Sea K/k una extensión cíclica de grado p^{n-1} . Sean $\langle\varphi\rangle = \text{Gal}(K/k)$, $o(\varphi) = p^{n-1}$, $\chi \in \mathbb{F}_p^* = \{1, \dots, p-1\}$ y $L = K(\theta)$ una extensión cíclica de grado p tal que L/k es una extensión cíclica de grado p^n . Sea $\langle\sigma\rangle = \text{Gal}(L/k)$, $o(\sigma) = p^n$ tal que $\varphi = \sigma \pmod{\text{Gal}(L/K)}$, es decir, $\varphi = \sigma|_K$. Sea $\sigma^{p^{n-1}} = \psi$, $\langle\psi\rangle = \text{Gal}(L/K)$.

$$\left. \begin{array}{c} L \\ \left| \begin{array}{c} \langle \psi \rangle \\ K \\ \left| \begin{array}{c} \langle \varphi \rangle \\ k \end{array} \right. \end{array} \right. \end{array} \right\} \langle \sigma \rangle \quad \text{Ahora, } L/K \text{ es una extensión cíclica de grado } p, \text{ es decir,}$$

una extensión de Artin-Schreier. Así, podemos escoger θ tal que $\wp\theta = \theta^p - \theta = \gamma \in K$ y tal que $\psi\theta = \theta + \chi$ o, equivalentemente, $(\psi - 1)\theta = \chi$. Se tiene que

$$(\psi - 1)(\sigma - 1)\theta = (\sigma - 1)(\psi - 1)\theta = (\sigma - 1)\chi = 0,$$

es decir, $\delta := (\sigma - 1)\theta \in K$. Además

$$(\varphi - 1)\gamma = (\varphi - 1)(\wp\theta) = (\sigma - 1)(\wp\theta) = \wp((\sigma - 1)\theta) = \wp\delta,$$

y se tiene

$$\begin{aligned} \text{Tr}_{K/k} \delta &= \sum_{i=0}^{p^{n-1}-1} \varphi^i \delta = \frac{\varphi^{p^{n-1}} - 1}{\varphi - 1} \delta = \frac{\sigma^{p^{n-1}} - 1}{\sigma - 1} (\sigma - 1)\theta \\ &= (\sigma^{p^{n-1}} - 1)\theta = (\psi - 1)\theta = \chi. \end{aligned}$$

En resumen, si L/k es una extensión cíclica de grado p^n que contiene a K , entonces existen $\theta \in L$, $\gamma \in K$, $\chi \in \{1, 2, \dots, p-1\}$ y $\delta \in K$ tales que si $\sigma|_K = \varphi$, $\sigma_{p^{n-1}} = \psi$, entonces

- (a) $\wp\theta = \gamma$,
- (b) $(\psi - 1)\theta = \chi$,
- (c) $(\sigma - 1)\theta = \delta$,
- (d) $(\varphi - 1)\gamma = \wp\delta$,
- (e) $\text{Tr}_{K/k} \delta = \chi$.

Recíprocamente, sea K/k una extensión cíclica de grado p^{n-1} . Como K/k es una extensión separable, existe $\delta \in K$ con $\text{Tr}_{K/k} \delta = \chi$, $\chi \in \mathbb{F}_p^*$. En particular,

$$\text{Tr}_{K/k} \wp(\delta) = \wp(\text{Tr}_{K/k} \delta) = \wp(\chi) = \chi^p - \chi = \chi - \chi = 0.$$

Por el Teorema 90 de Hilbert, existe $\gamma \in K$ tal que $(\varphi - 1)\gamma = \wp\delta$, donde $\langle \varphi \rangle = \text{Gal}(K/k)$. Si δ' es cualquier otro elemento tal que $\text{Tr}_{K/k} \delta' = \chi$, entonces $\text{Tr}_{K/k}(\delta' - \delta) = 0$. Nuevamente por el Teorema 90 de Hilbert, existe $\alpha \in K$ tal que $\delta' - \delta = (\varphi - 1)\alpha$. Se tiene $\delta' = \delta + (\varphi - 1)\alpha$. Al sustituir δ por $\delta' = \delta + (\varphi - 1)\alpha$, tenemos

$$\begin{aligned} (\varphi - 1)(\gamma + \wp\alpha) &= (\varphi - 1)\gamma + \wp((\varphi - 1)\alpha) = \wp\delta + \wp((\varphi - 1)\alpha) \\ &= \wp(\delta + (\varphi - 1)\alpha) = \wp\delta'. \end{aligned}$$

Es decir, la sustitución $\delta \leftrightarrow \delta + (\varphi - 1)\alpha$ corresponde a la sustitución $\gamma \leftrightarrow \gamma + \wp\alpha$, $\alpha \in K$.

Veamos que $\gamma \neq \wp\beta$ para $\beta \in K$. En caso contrario, si $\gamma = \wp\beta$ para algún $\beta \in K$, cambiando γ por $\gamma' = \gamma - \wp\beta = 0$, se tendría $(\varphi - 1)\gamma' = 0 = \wp\delta'$, esto es, $\delta' \in \mathbb{F}_p$ y $\text{Tr}_{K/k} \delta' = 0 = \chi$ lo cual es absurdo. Esto prueba que $\gamma \notin \wp(K)$.

Sea θ una solución de la ecuación $x^p - x - \gamma \in K[x]$, es decir, $\wp\theta = \gamma$, $\theta \notin K$. Sea $L = K(\theta)$. Se tiene $[L : k] = p^n$. Ahora, $\wp(\theta + \delta) = \wp\theta + \wp\delta = \gamma + (\varphi - 1)\gamma = \varphi\gamma$. Sea

$$\sigma: L \rightarrow L \quad \text{definida por} \quad \sigma\theta = \theta + \delta \quad \text{y} \quad \sigma|_K = \varphi.$$

Se tiene que

$$\begin{aligned} \sigma^{p^{n-1}}\theta - \theta &= (\sigma^{p^{n-1}} - 1)\theta = \left(\sum_{i=0}^{p^{n-1}-1} \sigma^i \right) (\sigma - 1)\theta \\ &= \left(\sum_{i=0}^{p^{n-1}-1} \sigma^i \right) \delta = \sum_{i=0}^{p^{n-1}-1} \varphi^i \delta = \text{Tr}_{K/k} \delta = \chi. \end{aligned}$$

Esto es, $\sigma^{p^{n-1}}\theta = \theta + \chi \neq \theta$ por lo que σ tiene orden p^n . Así, L/k es cíclica generada por σ . En resumen, tenemos

Teorema 11.2.4 (Witt [77]). *Sea K/k una extensión cíclica de grado p^{n-1} , $n \geq 2$. Entonces para construir cualquier extensión cíclica L/k de grado p^n que contenga a K , se eligen de manera arbitraria los siguiente:*

- (I) *Un generador φ de $\text{Gal}(K/k)$.*
- (II) *Un elemento $\chi \neq 0$ en \mathbb{F}_p , es decir, $\chi \in \{1, 2, \dots, p-1\}$.*
- (III) *Una solución $\delta \in K$ de la ecuación $\text{Tr}_{K/k} \delta = \chi$.*
- (IV) *Una solución $\gamma \in K$ de la ecuación $(\varphi - 1)\gamma = \wp\delta$.*

La extensión L se obtiene como $L = K(\theta)$ donde $\wp\theta = \gamma$. Cualquier otra extensión de este tipo se obtiene sustituyendo γ por $\gamma + c$ con $c \in k$. \square .

Este es el resultado clave usado por Schmid para generar extensiones cíclicas de grado p^n en característica p .

11.3. La construcción de Schmid

Sea k un campo arbitrario de característica p . Sea K_i una extensión cíclica de k de grado p^i con $\text{Gal}(K_i/k) = \langle \varphi_i \rangle$, $i = 1, 2, \dots, n$. Sea $T_i := \text{Tr}_{K_i/k}$. Suponemos $k \subseteq K_1 \subseteq \dots \subseteq K_n = L$. Seleccionamos $\chi = 1$ en el resultado de Witt (Teorema 11.2.4). Sea $c_i \in K_i$ un elemento tal que $T_i c_i = 1$ y como de costumbre sea $\wp x = x^p - x$. Sea Δ_i el operador $\varphi_i - 1$. La extensión

K_i/K_{i-1} está dada por $K_i = K_{i-1}(v_i)$, $i = 2, 3, \dots$ con $\wp v_i = z_{i-1} \in K_{i-1}$ y $\Delta_{i-1} z_{i-1} = \wp c_{i-1}$. Se tiene que $\varphi_i(v_i) = v_i + c_{i-1}$.

Consideremos el elemento $\alpha = -v_1^{p-1} \in K_1$. Sea $X_i := v_i + i$, $1 \leq i \leq p$. Sean σ_i las funciones simétricas elementales en X_1, \dots, X_p :

$$\sigma_0 = 1, \quad \sigma_1 = \sum_{i=1}^p X_i, \quad \sigma_2 = \sum_{i < j} X_i X_j, \quad \dots, \quad \sigma_p = X_1 \cdots X_p$$

y sean

$$\rho_m := X_1^m + \cdots + X_p^m \quad \text{para } m \geq 1 \quad \text{y} \quad \rho_0 = p = 0.$$

Se tiene

$$Y^p - Y - \beta_1 = \prod_{i=1}^p (Y - (v_i + i)) = \prod_{i=1}^p (Y - X_i) = \sum_{i=0}^p (-1)^i \sigma_i Y^{p-i},$$

por lo que $(-1)^p \prod_{i=1}^p X_i = -\beta_1$, esto es, $\sigma_1 = \cdots = \sigma_{p-2} = 0$, $\sigma_{p-1} = -1$ y $\sigma_p = \beta_1$.

Por las identidades de Newton

$$\rho_{p-1} - \rho_{p-2} \sigma_1 + \cdots + (-1)^{p-2} \rho_1 \sigma_{p-2} + (-1)^{p-1} \sigma_{p-1} (p-1) = 0$$

se obtiene $\rho_{p-1} = (-1)^{p-1} \sigma_{p-1} = (-1)^p = -1$. Por otro lado

$$\rho_{p-1} = \sum_{i=1}^p (v_i + i)^{p-1} = \text{Tr}_{K_1/k} v_1^{p-1} = -1.$$

Por lo tanto $\text{Tr}_{K_1/k}(-v_1^{p-1}) = 1$. Este es el δ correspondiente al Teorema 11.2.4 (III).

En el caso general consideramos $c_n := (-1)^n \prod_{i=1}^n v_i^{p-1}$, se tiene

$$\begin{aligned} \text{Tr}_{K_n/k} c_n &= \text{Tr}_{K_{n-1}/k} \text{Tr}_{K_n/K_{n-1}} \left\{ (-1)^n \prod_{i=1}^n v_i^{p-1} \right\} \\ &= \text{Tr}_{K_{n-1}/k} \left((-1)^n \prod_{i=1}^{n-1} v_i^{p-1} \text{Tr}_{K_n/K_{n-1}} v_n^{p-1} \right) \\ &= \text{Tr}_{K_{n-1}/k} \left((-1)^n \prod_{i=1}^{n-1} v_i^{p-1} (-1) \right) = \text{Tr}_{K_{n-1}/k} c_{n-1}. \end{aligned}$$

Por lo tanto, se sigue por inducción que $\text{Tr}_{K_n/k} c_n = 1$ y estos elementos sirven para la construcción. Schmid construyó en general las extensiones y probó que la extensión cíclica K_n/k en general está dada por

$$\begin{array}{llll}
K_1 = k(v_1), & \wp v_1 = \beta_1, & \Delta_1 v_1 = 1, & \\
K_2 = K_1(v_2), & \wp v_2 = z_1 + \beta_2, & \Delta_2 v_2 = c_1, & \Delta_1 z_1 = \wp c_1 \\
K_3 = K_2(v_3), & \wp v_3 = z_2 + \beta_3, & \Delta_3 v_3 = c_2, & \Delta_2 z_2 = \wp c_2 \\
\vdots & \vdots & \vdots & \vdots \\
K_n = K_{n-1}(v_n), & \wp v_n = z_{n-1} + \beta_n, & \Delta_n v_n = c_{n-1}, & \Delta_{n-1} z_{n-1} = \wp c_{n-1}
\end{array} \quad (11.1)$$

donde K_n está determinada por los elementos $\beta_1, \dots, \beta_n \in k$ arbitrarios, $\beta_1 \notin \wp(k)$ y donde $\Delta_i = \varphi_i - 1$, $\varphi_i(v_i) = v_i + c_{i-1}$, $\langle \varphi_i \rangle = \text{Gal}(K_i/k)$.

Las ecuaciones que encontró Schmid para generar las extensiones cíclicas fueron reconocidas por Witt en forma vectorial y esto dio lugar a los *vectores de Witt*.

11.4. Vectores de Witt

Sea p un número primo fijo. Para un vector $\mathbf{x} = (x_1, x_2, \dots)$ con una cantidad a lo más numerable de componentes x_n , en característica 0, se definen las *componentes fantasmas* de \mathbf{x} por

$$x^{(t)} = x_1^{p^{t-1}} + px_2^{p^{t-2}} + \dots + p^{t-1}x_t = \sum_{i=1}^t p^{i-1}x_i^{p^{t-i}}, \quad t = 1, 2, \dots \quad (11.2)$$

Recíprocamente, x_t puede ser calculado recursivamente como un polinomio en $x^{(1)}, x^{(2)}, \dots, x^{(t)}$ a partir de (11.2). Esta correspondencia puede ser expresada como

$$\mathbf{x} = (x_1, x_2, x_3, \dots \mid x^{(1)}, x^{(2)}, x^{(3)}, \dots).$$

La suma $\dot{+}$, la diferencia $\dot{-}$ y el producto $\dot{\times}$ de Witt se definen por

$$\mathbf{x} \dot{\pm} \mathbf{y} := (?, \dots \mid x^{(1)} \dot{\pm} y^{(1)}, x^{(2)} \dot{\pm} y^{(2)}, \dots). \quad (11.3)$$

Esto es, las componentes fantasma se operan término a término y las componentes usuales se calculan a partir de los resultados que se obtengan en las componentes fantasma.

Notemos que $(\mathbf{x})^{(n)}$ y $x^{(n)}$ denotan lo mismo, a saber, la n -componente fantasma del vector \mathbf{x} . Similarmente $(\mathbf{x})_n$ y x_n denotan lo mismo, la n -componente de \mathbf{x} .

Lo anterior puede precisarse de la siguiente forma. Consideremos tres familias $\{x_i, y_j, z_\ell\}_{i,j,\ell=1}^N$ donde $N \in \mathbb{N} \cup \{\infty\}$, de variables independientes sobre \mathbb{Q} y consideramos el anillo $R = \mathbb{Q}[x_i, y_j, z_\ell]_{i,j,\ell}$. Sea R^N el producto $\underbrace{R \times \dots \times R \times \dots}_N$. Por abuso del lenguaje, denotamos por R^N al anillo que

como conjunto base tiene al mismo conjunto R^N y cuyas operaciones son término a término (esto corresponde a las componentes fantasma) y sea R_N el anillo que como conjunto sigue siendo R^N pero con las *operaciones de Witt*: sea $\varphi: R_N \rightarrow R^N$ dado por $\varphi(a_1, a_2, \dots, a_N) = (a^{(1)}, a^{(2)}, \dots, a^{(N)})$ donde

$$a^{(m)} := a_1^{p^{m-1}} + pa_2^{p^{m-2}} + \dots + p^{m-1}a_m, \quad m = 1, 2, \dots, N.$$

Se tiene que φ es un mapeo biyectivo y el inverso $\psi: R^N \rightarrow R_N$ está dado por $\psi(a^{(1)}, a^{(2)}, \dots, a^{(N)}) = (a_1, a_2, \dots, a_N)$ donde

$$a_m := \frac{1}{p^{m-1}}(a^{(m)} - a_1^{p^{m-1}} - pa_2^{p^{m-2}} - \dots - p^{m-2}a_{m-1}^p), \quad m = 1, \dots, N.$$

Entonces las operaciones $\dot{+}, \dot{-}, \dot{\times}$ sobre R^N se definen por

$$\mathbf{a} \dot{\pm}_{\times} \mathbf{b} := (\mathbf{a}^{\varphi} \pm_{\times} \mathbf{b}^{\varphi})^{\varphi^{-1}} = (\mathbf{a}^{\varphi} \pm_{\times} \mathbf{b}^{\varphi})^{\psi}. \quad (11.4)$$

En otras palabras, dados dos vectores en R_N , los trasladamos a R^N y ahí los operamos de la manera usual, es decir, componente por componente y al resultado lo volvemos a R_N . Como R^N es conmutativo con unidad, R_N también es conmutativo con unidad. Por ejemplo si $N = 2$, entonces dados \mathbf{x}, \mathbf{y}

$$\begin{aligned} \mathbf{x} &= (x_1, x_2 \mid x^{(1)}, x^{(2)}) = (x_1, x_2 \mid x_1, x_1^p + px_2), \\ \mathbf{y} &= (y_1, y_2 \mid y^{(1)}, y^{(2)}) = (y_1, y_2 \mid y_1, y_1^p + py_2), \end{aligned}$$

se tiene que

$$\begin{aligned} \mathbf{z} = \mathbf{x} \dot{+} \mathbf{y} &= (z_1, z_2 \mid z^{(1)}, z^{(2)}) = (z_1, z_2 \mid z_1, z_1^p + pz_2) \\ &= (?, ? \mid x_1 + y_1, x_1^p + px_2 + y_1^p + py_2). \end{aligned}$$

Esto es $z_1 = x_1 + y_1, z_1^p = x_1^p + y_1^p + pz_2$. Por lo tanto

$$\begin{aligned} z_2 &= \frac{1}{p}(x_1^p + px_2 + y_1^p + py_2 - (x_1 + y_1)^p) \\ &= \frac{1}{p}(px_2 + py_2 - \sum_{i=2}^{p-1} \binom{p}{i} x_1^i y_1^{p-i}) = x_2 + y_2 - \sum_{i=2}^{p-1} \frac{1}{p} \binom{p}{i} x_1^i y_1^{p-i}. \end{aligned}$$

Por lo tanto

$$\mathbf{z} = \mathbf{x} \dot{+} \mathbf{y} = (x_1 + y_1, x_2 + y_2 - \sum_{i=2}^{p-1} \frac{1}{p} \binom{p}{i} x_1^i y_1^{p-i} \mid x_1 + y_1, x_1^p + px_2 + y_1^p + py_2).$$

A continuación introducimos las siguientes operaciones en los vectores de Witt que son de gran utilidad para obtener información de la naturaleza del anillo R_N .

Definición 11.4.1. Se define el *operador de corrimiento* $V: R_N \rightarrow R_N$ por

$$\begin{aligned} V(x_1, \dots, x_n, \dots) &= (0, x_1, \dots, x_n, \dots), \\ V^i(x_1, \dots, x_n, \dots) &= (0, \dots, 0, \underbrace{x_1}_{i+1}, \dots, x_n, \dots), \quad i \in \mathbb{N}, \end{aligned}$$

y se define la *función componente* $\{ \}: R \rightarrow R_N$,

$$\begin{aligned} \{u\} &:= (u, 0, \dots, 0, \dots) = (u, 0, \dots, 0, \dots \mid u, u^p, u^{p^2}, \dots), \\ \{u\}^{(n)} &= u^{p^{n-1}}, \quad n \geq 1, \quad \text{y} \quad u_1 = u, \quad u_n = 0, \quad n \geq 2. \end{aligned}$$

Se tiene $V^i(\{u\}) = (0, \dots, 0, \underbrace{u}_{i+1}, 0, \dots)$.

Observación 11.4.2. Se tiene

$$(V\mathbf{x})^{(n)} = px^{(n-1)}, \quad n = 1, 2, \dots, \quad \text{donde} \quad x^{(0)} = 0. \quad (11.5)$$

En efecto $(V\mathbf{x})^{(n)} = (0, x_1, \dots, x_m, \dots)^{(n)} = 0^{p^{n-1}} + px_1^{p^{n-2}} + \dots + p^{n-1}x_{n-1}$ y $x^{(n-1)} = x_1^{p^{n-2}} + px_2^{p^{n-3}} + \dots + p^{n-2}x_{n-1}$, de donde se sigue la igualdad.

En otras palabras tenemos

$$V\mathbf{x} = (0, x_1, x_2, \dots \mid 0, px^{(1)}, px^{(2)}, \dots). \quad (11.6)$$

Para $s = 0, 1, 2, \dots$ se tiene

$$V^s\mathbf{x} = (\underbrace{0, \dots, 0}_s, x_1, x_2, \dots \mid 0, \dots, 0, p^s x^{(1)}, p^s x^{(2)}, \dots) \quad (11.7)$$

donde $V^0 = \text{Id}$, es decir, $V^0\mathbf{x} = \mathbf{x}$ para toda $\mathbf{x} \in R^N$. En particular

$$(V^s\mathbf{x})^{(n)} = \begin{cases} 0 & \text{si } s \leq n \\ p^s x^{(n-s)} & \text{si } n \geq s+1 \end{cases} = p^s x^{(n-s)}$$

donde $x^{(1-s)} = \dots = x^{(-1)} = x^{(0)} = 0$. Esta última igualdad puede ser verificada por inducción en s :

$$\begin{aligned} (V^s\mathbf{x})^{(n)} &= (V(V^{s-1}\mathbf{x}))^{(n)} = p(V^{s-1}\mathbf{x})^{(n-1)} \\ &= p(p^{s-1}x^{(n-1-(s-1))}) = p^s x^{(n-s)}, \\ x^{(1-s)} &= x^{(2-s)} = \dots = x^{(-1)} = x^{(0)} = 0. \end{aligned}$$

Aplicado lo anterior a $\{u\}$ se tiene la igualdad

$$(V^s\{u\})^{(n)} = p^s \{u\}^{(n-s)} = \begin{cases} p^s u^{p^{n-s-1}} & \text{si } n \geq s+1 \\ 0 & \text{si } n \leq s \end{cases}.$$

Proposición 11.4.3. Para $\mathbf{x}, \mathbf{y} \in R_N$, $u \in R$ se tiene

$$V(\mathbf{x} \dot{+} \mathbf{y}) = V\mathbf{x} \dot{+} V\mathbf{y}, \quad (11.8)$$

$$\mathbf{x} = (x_1, x_2, \dots) = \sum_{j=0}^r V^j(\{x_{j+1}\}) \dot{+} V^{r+1}(x_{r+2}, x_{r+3}, \dots), \quad (11.9)$$

$$\{u\}(x_1, x_2, \dots, x_n, \dots) = (ux_1, u^p x_2, \dots, u^{p^{n-1}} x_n, \dots). \quad (11.10)$$

Demostración. Puesto que $\mathbf{x} = \mathbf{y}$ si y sólo si $x^{(n)} = y^{(n)}$ para toda $n \in \mathbb{N}$, basta verificar que las n -componentes fantasma coinciden.

- (I) $(V(\mathbf{x} \dot{+} \mathbf{y}))^{(n)} = p(x+y)^{(n-1)} = p(x^{(n-1)} + y^{(n-1)}) = px^{(n-1)} + py^{(n-1)} = (V\mathbf{x})^{(n)} + (V\mathbf{y})^{(n)}$ de donde $V(\mathbf{x} \dot{+} \mathbf{y}) = V\mathbf{x} \dot{+} V\mathbf{y}$.
 (II) Se tiene

$$\begin{aligned} & \left(\sum_{j=0}^r V^j(\{x_{j+1}\}) + V^{r+1}(x_{r+2}, x_{r+3}, \dots) \right)^{(n)} \\ &= \sum_{j=0}^r (V^j(\{x_{j+1}\}))^{(n)} + (V^{r+1}(x_{r+2}, x_{r+3}, \dots))^{(n)} \\ &= \sum_{j=0}^r (V^j(\{x_{j+1}\}))^{(n)} + p^{r+1}(x_{r+2}, x_{r+3}, \dots)^{(n-(r+1))} = A. \end{aligned}$$

Para $n = 1, 2, \dots, r+1$, $0 \leq j \leq r$,

$$(V^j(\{x_{j+1}\}))^{(n)} = (p^j \{x_{j+1}\})^{(n-j)} = \begin{cases} p^j x_{j+1}^{p^{n-j-1}}, & n \geq j+1, \\ 0, & n \leq j, \end{cases}$$

y $p^{r+1}(x_{r+2}, x_{r+3}, \dots)^{(n-(r+1))} = 0$.

Por tanto, para $n = 1, 2, \dots, r+1$, se tiene $A = \sum_{j=0}^{n-1} p^j x_{j+1}^{p^{n-j-1}} = \sum_{j=1}^n p^{j-1} x_j^{p^{n-j}} = x^{(n)}$.

Ahora bien, para $n \geq r+2$, $(V^j(\{x_{j+1}\}))^{(n)} = p^j x_{j+1}^{p^{n-j-1}}$, $j = 0, 1, \dots, r$ y

$$\begin{aligned} p^{r+1}(x_{r+2}, x_{r+3}, \dots)^{(n-(r+1))} &= p^{r+1}(x_{r+2}, x_{r+3}, \dots)^{(n-r-1)} \\ &= p^{r+1} \left(\sum_{i=1}^{n-r-1} p^{i-1} x_{r+1+i}^{p^{n-r-1-i}} \right) \\ &= \sum_{i=1}^{n-r-1} p^{r+i} x_{r+1+i}^{p^{n-r-1-i}} \quad i \leftrightarrow r+1+i \\ &= \sum_{i=r+2}^n p^{i-1} x_i^{p^{n-i}}. \end{aligned}$$

Por tanto

$$\begin{aligned} A &= \sum_{j=0}^r p^j x_{j+1}^{p^{n-j-1}} + \sum_{j=r+2}^n p^{j-1} x_j^{p^{n-j}} = \sum_{j=1}^{r+1} p^{j-1} x_j^{p^{n-j}} + \sum_{j=r+2}^n p^{j-1} x_j^{p^{n-j}} \\ &= \sum_{j=1}^n p^{j-1} x_j^{p^{n-j}} = x^{(n)}. \end{aligned}$$

Se sigue (11.9).

(III) Se tiene que $(\{u\}(x_1, x_2, \dots, x_n \dots))^{(n)} = \{u\}^{(n)}(x_1, x_2, \dots)^{(n)} = u^{p^{n-1}} x^{(n)}$. Por otro lado

$$\begin{aligned} (ux_1, u^p x_2, \dots, u^{p^{n-1}} x_{n-1}, \dots)^{(n)} &= \sum_{j=1}^n p^{j-1} (u^{p^{j-1}} x_j)^{p^{n-j}} \\ &= u^{p^{n-1}} \sum_{j=1}^n p^{j-1} x_j^{p^{n-j}} = u^{p^{n-1}} x^{(n)}. \end{aligned}$$

Se sigue (11.10). \square

Notación 11.4.4. Para $m \in \mathbb{N} \cup \{0\}$, se denota

$$\mathbf{0} := (0, 0, \dots, 0, \dots), \quad \mathbf{1} := (1, 0, \dots, 0, \dots), \quad \mathbf{m} = m\mathbf{1} := \underbrace{\mathbf{1} \dot{+} \mathbf{1} \dot{+} \dots \dot{+} \mathbf{1}}_{m \text{ veces}}. \quad (11.11)$$

Sea p un número primo, $\mathbf{x} = (x_1, \dots, x_n, \dots)$. Se define

$$F(\mathbf{x}) = \mathbf{x}^p := (x_1^p, \dots, x_n^p, \dots). \quad (11.12)$$

Observemos que \mathbf{x}^p no es la p -potencia de la multiplicación de Witt, es decir $\mathbf{x}^p \neq \underbrace{\mathbf{x} \times \mathbf{x} \times \dots \times \mathbf{x}}_p$.

Definición 11.4.5. Al homomorfismo F se la llama el *automorfismo de Frobenius* en R_N .

Observemos que

$$x^{(n)} = \sum_{j=1}^n p^{j-1} x_j^{p^{n-j}} = \sum_{j=1}^{n-1} p^{j-1} (x_j^p)^{p^{n-1-j}} + p^{n-1} x_n = (x^p)^{(n-1)} + p^{n-1} x_n.$$

Esto es

$$x^{(n)} = (x^p)^{(n-1)} + p^{n-1} x_n, \quad n = 1, 2, \dots, \quad (x^p)^{(0)} = 0. \quad (11.13)$$

Observemos que $(x^p)^{(n-1)}$ denota la $(n-1)$ -componente fantasma de x^p y no la $p(n-1)$ potencia x . De (11.4), obtenemos que si $I = \mathbb{Z}[x_i, y_j, z_k]$, entonces

$$p^{n-1}(x+y)_n \equiv (x+y)^{(n)} \pmod{I} = (x^{(n)} + y^{(n)}) \equiv p^{n-1}x_n + p^{n-1}y_n \pmod{I}.$$

Por tanto existe $f \in I$, tal que

$$(x+y)_n = x_n + y_n + f(x_1, y_1, \dots, x_{n-1}, y_{n-1}). \quad (11.14)$$

11.5. Aritmética de los vectores de Witt

Sea \mathfrak{F} un dominio entero de característica 0, de tal forma que $\mathbb{Z} \subseteq \mathfrak{F}$. Sea $p \in \mathbb{Z}$ un número primo.

Lema 11.5.1. *Sean \mathbf{x}, \mathbf{y} dos vectores cuyas componentes regulares están en \mathfrak{F} . Entonces para $r > 0$, se tienen que las congruencias*

$$x_n \equiv y_n \pmod{p^r \mathfrak{F}} \quad y \quad x^{(n)} \equiv y^{(n)} \pmod{p^{r+n-1} \mathfrak{F}}$$

son equivalentes.

Demostración. Procedemos por inducción en n . Si para $n-1$ se tiene la equivalencia, entonces si $x_n \equiv y_n \pmod{p^r \mathfrak{F}}$, entonces $(x^p)_n = x_n^p \equiv y_n^p = (y^p)_n \pmod{p^{r+1} \mathfrak{F}}$ por lo que $(x^p)^{(n-1)} \equiv (y^p)^{(n-1)} \pmod{p^{r+n-1} \mathfrak{F}}$.

Ahora, por (11.13), $x^{(n)} = (x^p)^{(n-1)} + p^{n-1}x_n$, entonces

$$(x^{(n)} - y^{(n)}) - (p^{n-1}x_n - p^{n-1}y_n) = (x^p)^{(n-1)} - (y^p)^{(n-1)} \pmod{p^{r+n-1} \mathfrak{F}}.$$

Por lo tanto $x^{(n)} \equiv y^{(n)} \pmod{p^{r+n-1} \mathfrak{F}} \iff p^{n-1}x_n - p^{n-1}y_n \equiv 0 \pmod{p^{r+n-1} \mathfrak{F}} \iff x_n \equiv y_n \pmod{p^r \mathfrak{F}}$. \square

Como consecuencia inmediata del Lema 11.5.1 tenemos:

Teorema 11.5.2. *Se tiene que $(\mathbf{x} \overset{\bullet}{\pm} \mathbf{y})_n \in \mathbb{Z}[x_1, y_1, \dots, x_{n-1}, y_{n-1}, x_n, y_n]$, $n = 1, 2, \dots$*

Demostración. Por definición $x^{(n)}, y^{(n)} \in \mathfrak{F} = \mathbb{Z}[x_1, y_1, \dots, x_n, y_n]$. Ahora bien, puesto que por (11.13) se tiene $x^{(n)} \equiv (x^p)^{(n-1)} \pmod{p^{n-1} \mathfrak{F}}$ y $y^{(n)} \equiv (y^p)^{(n-1)} \pmod{p^{n-1} \mathfrak{F}}$, se sigue que $(\mathbf{x} \overset{\bullet}{\pm} \mathbf{y})^{(n)} = x^{(n)} \overset{\pm}{\pm} y^{(n)} \equiv (x^p)^{(n-1)} \overset{\pm}{\pm} (y^p)^{(n-1)} \pmod{p^{n-1} \mathfrak{F}}$.

Por inducción, si para $j < n$ el teorema ya está demostrado, entonces $(\mathbf{x} \overset{\bullet}{\pm} \mathbf{y})_j^p \equiv (x^p \pm y^p)_j \pmod{p \mathfrak{F}}$. Por el Lema 11.5.1 para $n-1$,

$$((\mathbf{x} \overset{\bullet}{\pm} \mathbf{y})^p)^{(n-1)} \equiv (x^p \pm y^p)^{(n-1)} \pmod{p^{n-1} \mathfrak{F}}.$$

Así $p^{n-1}(\mathbf{x} \dot{\pm}_{\times} \mathbf{y})_n = (\mathbf{x} \dot{\pm}_{\times} \mathbf{y})^{(n)} - ((\mathbf{x} \dot{\pm}_{\times} \mathbf{y})^p)^{(n-1)} \equiv 0 \pmod{p^{n-1}\mathfrak{F}}$, de donde se sigue que $\mathbf{x} \dot{\pm}_{\times} \mathbf{y} \in \mathfrak{F}$. \square

Cuando estudiemos la acción de Galois, necesitaremos el siguiente resultado.

Teorema 11.5.3. *Se tiene que, por componentes,*

$$\mathbf{p}\mathbf{x} \equiv V\mathbf{x}^p \pmod{p\mathbb{Z}[x_1, x_2, \dots]},$$

es decir $(\mathbf{p}\mathbf{x})_n \equiv (V\mathbf{x}^p)_n \pmod{p\mathbb{Z}[x_1, x_2, \dots]}$.

Demostración. Por (11.13), (11.5) y (11.3) se tiene que las componentes fantasma satisfacen

$$\begin{aligned} (\mathbf{p}\mathbf{x})^{(n)} &= px^{(n)} \equiv p(\mathbf{x}^p)^{(n-1)} + p^n x_n \equiv p(\mathbf{x}^p)^{(n-1)} \\ &\equiv (V\mathbf{x}^p)^{(n)} \pmod{p^n\mathbb{Z}[x_1, \dots, x_n, \dots]}. \end{aligned}$$

Por el Lema 11.5.1, con $r = 1$, se obtiene

$$(\mathbf{p}\mathbf{x})_n = (V\mathbf{x}^p)_n \pmod{p\mathbb{Z}[x_1, \dots, x_n, \dots]}. \quad \square$$

11.6. Vectores de Witt en característica p

Hasta ahora hemos considerado las operaciones de Witt en característica 0 pues al pasar de las componentes fantasma a las componentes de Witt, se está dividiendo entre una potencia de p . Esto es, con la notación de (11.4)

$$\mathbf{a} \dot{\pm}_{\times} \mathbf{b} = (\mathbf{a}^{\varphi} \pm \mathbf{b}^{\varphi})^{\varphi^{-1}} = (\mathbf{a}^{\varphi} \pm \mathbf{b}^{\varphi})^{\psi}$$

lo cual hace de R_N un anillo pues todas las reglas se cumplen en R^N y son transformadas a R_N bajo φ^{-1} . Por ejemplo

$$\begin{aligned} (\mathbf{a} \dot{+} \mathbf{b}) \dot{+} \mathbf{c} &= (\mathbf{a}^{\varphi} + \mathbf{b}^{\varphi})^{\varphi^{-1}} \dot{+} \mathbf{c} = \left(((\mathbf{a}^{\varphi} + \mathbf{b}^{\varphi})^{\varphi^{-1}})^{\varphi} + \mathbf{c}^{\varphi} \right)^{\varphi^{-1}} \\ &= ((\mathbf{a}^{\varphi} + \mathbf{b}^{\varphi}) + \mathbf{c}^{\varphi})^{\varphi^{-1}} = (\mathbf{a}^{\varphi} + (\mathbf{b}^{\varphi} + \mathbf{c}^{\varphi}))^{\varphi^{-1}} \\ &= \left(\mathbf{a}^{\varphi} + ((\mathbf{b}^{\varphi} + \mathbf{c}^{\varphi})^{\varphi^{-1}})^{\varphi} \right)^{\varphi^{-1}} \\ &= \left(\mathbf{a}^{\varphi} + (\mathbf{b} \dot{+} \mathbf{c})^{\varphi} \right)^{\varphi^{-1}} = \mathbf{a} \dot{+} (\mathbf{b} \dot{+} \mathbf{c}). \end{aligned}$$

Por el Teorema 11.5.3 las operaciones de Witt pueden hacerse módulo p y de esta forma obtenemos

Teorema 11.6.1. Sea k un campo de característica p y sea $W_N(k)$ el anillo de Witt

$$W_N(k) := \{(x_1, \dots, x_n, \dots) \mid x_i \in k\}, \quad N \in \mathbb{N} \cup \{\infty\}.$$

Entonces $W_N(k)$ es un anillo conmutativo con unidad y se tiene para $\mathbf{x}, \mathbf{y} \in W_N(k)$

$$(\mathbf{x} \dot{+} \mathbf{y})^p = \mathbf{x}^p \dot{+} \mathbf{y}^p. \quad (11.15)$$

$$\mathbf{p} \dot{\times} \mathbf{x} = \mathbf{p}\mathbf{x} = V\mathbf{x}^p = (V\mathbf{x})^p. \quad (11.16)$$

$$(V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) = V^{i+j}(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}^{p^i}). \quad (11.17)$$

Demostración. Todas las propiedades de anillo se cumplen formalmente por lo que $W_N(k)$ es un anillo. Ahora bien, se tiene que (11.15) se sigue del Lema 11.5.1 y de (11.13):

$$\begin{aligned} ((\mathbf{x} \dot{+} \mathbf{y})^p \dot{-} \mathbf{x}^p \dot{-} \mathbf{y}^p)^{(n)} &= ((\mathbf{x} \dot{+} \mathbf{y})^p)^{(n)} - (\mathbf{x}^p)^{(n)} - (\mathbf{y}^p)^{(n)} \\ &= (\mathbf{x} \dot{+} \mathbf{y})^{(n+1)} - p^n(\mathbf{x} \dot{+} \mathbf{y})_n - x^{(n+1)} + p^n x_n - y^{(n+1)} + p^n y_n. \end{aligned}$$

Puesto que $(\mathbf{x} \dot{+} \mathbf{y})^{(n+1)} = x^{(n+1)} + y^{(n+1)}$, se sigue que $((\mathbf{x} \dot{+} \mathbf{y})^p \dot{-} \mathbf{x}^p \dot{-} \mathbf{y}^p)^{(n)} \equiv 0 \pmod{p^n} = 0 \pmod{p^{1+(n-1)}}$. Por el Lema 11.5.1 se sigue $(\mathbf{x} \dot{+} \mathbf{y})^p = \mathbf{x}^p \dot{+} \mathbf{y}^p$. Similarmente $(\mathbf{x} \dot{-} \mathbf{y})^p = \mathbf{x}^p \dot{-} \mathbf{y}^p$ y $(\mathbf{x} \dot{\times} \mathbf{y})^p = \mathbf{x}^p \dot{\times} \mathbf{y}^p$.

Se tiene que (11.16) es el Teorema 11.5.3. Además tenemos por (11.5) y (11.13) que

$$((V\mathbf{x})^p)^{(n)} = (V\mathbf{x})^{(n+1)} - p^n x_{n+1} = px^{(n)}$$

y

$$(V\mathbf{x}^p)^{(n)} = p(\mathbf{x}^p)^{(n-1)} = p(x^{(n)} - p^{n-1}x_n)$$

de donde se obtiene

$$((V\mathbf{x})^p)^{(n)} \equiv (V\mathbf{x}^p)^{(n)} \pmod{p^n}.$$

Por el Lema 11.5.1 obtenemos que

$$(V\mathbf{x})_n^p \equiv (V\mathbf{x}^p)_n \pmod{p}.$$

Por lo tanto

$$F \circ V = V \circ F = \mathbf{p}.$$

Para probar (11.17) notemos primero que de (11.13) obtenemos

$$\begin{aligned} (\mathbf{x}^p)^{(n)} &= x^{(n+1)} - p^n x_n \equiv x^{(n+1)} \pmod{p^n}, \\ (\mathbf{x}^{p^2})^{(n)} &= (\mathbf{x}^p)^{(n+1)} - p^n (\mathbf{x}^p)_n \\ &= x^{(n+2)} - p^{n+1} x_{n+1} - p^n (\mathbf{x}^p)_n \equiv x^{(n+2)} \pmod{p^n}. \end{aligned}$$

En general obtenemos

$$(\mathbf{x}^{p^j})^{(n)} \equiv x^{(n+j)} \pmod{p^n}.$$

Ahora para $i = 0, j = 0$ se tiene

$$(V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) = (V^0 \mathbf{x}) \dot{\times} (V^0 \mathbf{y}) = \mathbf{x} \dot{\times} \mathbf{y} = V^{0+0}(\mathbf{x}^{p^0} \dot{\times} \mathbf{y}^{p^0}),$$

por lo que se cumple (11.17) para $i = j = 0$.

Para $i = 0, j \geq 1$ se tiene

$$(V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) = V^0(\mathbf{x}) \dot{\times} V^j(\mathbf{y}) = \mathbf{x} \dot{\times} V^j \mathbf{y}$$

y

$$V^{i+j}(\mathbf{x}^{p^j} \mathbf{y}^{p^i}) = V^j(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}).$$

Se sigue que

$$\begin{aligned} (\mathbf{x} \dot{\times} V^j \mathbf{y})^{(n)} &= x^{(n)} (V^j \mathbf{y})^{(n)} = p^j x^{(n)} y^{(n-j)}, \\ (V^j(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}))^{(n)} &= p^j ((\mathbf{x}^{p^j}) \dot{\times} \mathbf{y})^{(n-j)} = p^j (\mathbf{x}^{p^j})^{(n-j)} y^{(n-j)} \\ &\equiv p^j x^{(n)} y^{(n-j)} \pmod{p^n}. \end{aligned}$$

Por lo tanto $(\mathbf{x} V^j \mathbf{y})_n \equiv (V^j(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}))_n \pmod{p}$ lo cual implica que $(V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) = V^{i+j}(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}^{p^i})$ para $i = 0, j \geq 1$.

Para $i \geq 1, j = 0$, $(V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) = (V^j \mathbf{y}) \dot{\times} (V^i \mathbf{x}) = V^{j+i}(\mathbf{y}^{p^i} \dot{\times} \mathbf{x}^{p^j}) = V^{i+j}(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}^{p^i})$.

Para el caso $i \geq 1, j \geq 1$, de la relación $V \mathbf{x}^p = \mathbf{p} \mathbf{x}$, se tiene

$$(V^j \mathbf{x}^p) = V(V^{j-1} \mathbf{x}^p) = \mathbf{p}(V^{j-1} \mathbf{x}^p) = \mathbf{p}^2(V^{j-2} \mathbf{x}^p) = \dots = \mathbf{p}^{j-1} V \mathbf{x}^p = \mathbf{p}^j \mathbf{x},$$

de donde

$$\begin{aligned} (V^i \mathbf{x}) \dot{\times} (V^j \mathbf{y}) &= (V^{i-1}(V \mathbf{x})) \dot{\times} (V^j \mathbf{y}) = V^{i+j-1}((V \mathbf{x})^{p^j} \dot{\times} \mathbf{y}^{p^{i-1}}) \\ &= V^{i+j-1}((V(\mathbf{x}^{p^j})) \dot{\times} \mathbf{y}^{p^{i-1}}) = V^{i+j-1}((V \mathbf{x}^{p^j}) \dot{\times} (V^0 \mathbf{y}^{p^{i-1}})) \\ &= V^{i+j-1}(V \mathbf{x}^{p^j} \dot{\times} (\mathbf{y}^{p^{i-1}})^p) = V^{i+j}(\mathbf{x}^{p^j} \dot{\times} \mathbf{y}^{p^i}). \quad \square \end{aligned}$$

Como veremos posteriormente, el siguiente resultado nos permite obtener el análogo al Teorema 11.2.1 para $n \in \mathbb{N}$ (el Teorema 11.2.1 es el caso $n = 1$).

Teorema 11.6.2. *En el anillo $W_N(k)$, donde k es un campo de característica p , se tiene que el vector $\mathbf{a} = (a_1, \dots, a_n, \dots) \in W_N(k)$ es invertible si y sólo si $a_1 \neq 0$.*

Demostración. Se tiene que $\{a_1^{-1}\} \dot{\times} \mathbf{a} = (1, y_1, \dots)$. Por tanto $\mathbf{1} \dot{-} \mathbf{a} \dot{\times} \{a_1^{-1}\} = V\mathbf{y}$ para algún $\mathbf{y} \in W_N(k)$. Sea $(V\mathbf{y})^i$ la i -ésima potencia de $V\mathbf{y}$ en $W_N(k)$, es decir, $(V\mathbf{y})^i = \underbrace{V\mathbf{y} \dot{\times} V\mathbf{y} \dot{\times} \dots \dot{\times} V\mathbf{y}}_i$. Entonces

$$\begin{aligned} \mathbf{a} \dot{\times} \{a_1^{-1}\} \dot{\times} \sum_{j=0}^{\infty} (V\mathbf{y})^j &= (\mathbf{1} \dot{-} V\mathbf{y}) \dot{\times} \sum_{j=0}^{\infty} (V\mathbf{y})^j \\ &= \sum_{j=0}^{\infty} (V\mathbf{y})^j \dot{-} \sum_{j=1}^{\infty} (V\mathbf{y})^j = (V\mathbf{y})^0 = \mathbf{1} \end{aligned}$$

y por tanto \mathbf{a} es invertible y de hecho se tiene $\mathbf{a}^{-1} = \{a_1^{-1}\} \dot{\times} \sum_{j=0}^{\infty} (V\mathbf{y})^j$.

El recíproco es inmediato pues existe $\mathbf{b} \in W_N(k)$ tal que $\mathbf{a} \dot{\times} \mathbf{b} = (a_1 b_1, \dots) = \mathbf{1} = (1, 0, \dots)$, esto es, $a_1 b_1 = 1$ y en particular $a_1 \neq 0$. \square

De la demostración del Teorema 11.6.1, obtenemos

$$\mathbf{p}^j \dot{\times} \mathbf{1} = V^j(\mathbf{1}^p) = (\underbrace{0, \dots, 0}_j, 1, 0, \dots), \quad j \in \mathbb{N}. \quad (11.18)$$

Ejemplo 11.6.3. Consideremos $N = n \in \mathbb{N}$ y $W_n(\mathbb{F}_p)$. Notemos que $\mathbf{1} \in W_n(\mathbb{F}_p)$ y se tiene de (11.18) que $\mathbf{p}^n = \mathbf{p}^n \dot{\times} \mathbf{1} = \mathbf{0}$ pero $\mathbf{p}^{n-1} = \mathbf{p}^{n-1} \dot{\times} \mathbf{1} \neq \mathbf{0}$. Además se tiene que $|W_n(\mathbb{F}_p)| = p^n$, lo cual implica que, como grupo con la adición de Witt, $W_n(\mathbb{F}_p)$ es cíclico de orden p^n . Más aún, $\varphi: \mathbb{Z} \rightarrow W_n(\mathbb{F}_p)$, $1 \mapsto \mathbf{1}$, es un epimorfismo de anillos con núc $\varphi(p^n)$, se sigue que $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ como anillos.

En particular tenemos que $W_n(\mathbb{F}_p)$ es de característica p^n . Por otro lado, las unidades de $W_n(\mathbb{F}_p)$ son precisamente $\{\mathbf{i} \mid 1 \leq i \leq p^n - 1, \text{mcd}(i, p) = 1\}$.

Ejemplo 11.6.4. En el caso $N = \infty$ se tiene que $W_N(\mathbb{F}_p)$ es un anillo de característica 0 pues para toda n , $\mathbf{p}^n = \mathbf{p}^n \dot{\times} \mathbf{1} = (0, \dots, 0, \underbrace{1}_{n+1}, 0, \dots) \neq 0$ y

si $\text{mcd}(i, p) = 1$, $i \in \mathbb{N}$, \mathbf{i} es unidad pues $i = \sum_{j=0}^m a_j p^j$, $a_j \in \{0, 1, \dots, p-1\}$ y $a_1 \neq 0$.

De hecho se tiene que $W_\infty(\mathbb{F}_p) \cong \mathbb{Z}_p$, \mathbb{Z}_p el anillo de los enteros p -ádicos.

Proposición 11.6.5. *Sea k un campo de característica p . Entonces $W_N(k)$ es de característica p^n si $N = n \in \mathbb{N}$ y 0 si $N = \infty$.*

Demostración. Igual que la de los Ejemplos 11.6.3 y 11.6.4. \square

11.7. Extensiones cíclicas de grado p^n en característica p

Usando los vectores de Witt, se tiene una teoría para p -extensiones cíclicas finitas paralela a la Teoría de Artin-Schreier para extensiones cíclicas de grado p en característica p y siendo esta última a su vez una teoría paralela a la Teoría de Kummer. Esta teoría recibe con frecuencia el nombre de *Teoría Aditiva de Kummer*.

En el caso de una extensión cíclica L/K en característica p de grado p^n con $n = 1$, Artin y Schreier probaron que toda tal extensión está dada por un ecuación del tipo $\wp y = x$, donde $\wp y := y^p - y$ y $x \in K, x \notin \wp(K) = \{a^p - a \mid a \in K\}$ (Teorema 11.2.1). La demostración se basa en que si un elemento $z \in L$ satisface $\text{Tr}_{L/K} z = 0$, entonces existe $w \in L$ tal que $(\sigma - 1)w = z$ donde $\langle \sigma \rangle = \text{Gal}(L/K)$, aunque la demostración original de Artin-Schreier, que es la que presentamos nosotros, no lo hizo de esta forma. Esto mismo se cumple prácticamente palabra por palabra para extensiones cíclicas de grado p^n usando el lenguaje de los vectores de Witt.

Sea K un campo arbitrario de característica p y consideremos $W_n(K) = \{(x_1, \dots, x_n) \mid x_i \in K\}$ el anillo de los vectores de Witt de longitud n con coeficientes en K . Sea L/K una extensión finita de Galois con grupo de Galois $G = \text{Gal}(L/K)$.

Definición 11.7.1. Si $\mathbf{y} \in W_n(L)$, $\mathbf{y} = (y_1, \dots, y_n)$, se define para $\sigma \in G$,

$$\sigma \mathbf{y} := (\sigma y_1, \dots, \sigma y_n) = \mathbf{y}^\sigma$$

y la traza $\text{Tr}_{L/K}: W_n(L) \rightarrow W_n(K)$ se define por

$$\text{Tr}_{L/K} \mathbf{y} = \sum_{\sigma \in G} \sigma \mathbf{y} = (\text{Tr}_{L/K} y_1, ?, \dots, ?) \in W_n(K).$$

Si $y_1 \in L$ es tal que $\text{Tr}_{L/K} y_1 \neq 0$, $\text{Tr}_{L/K} \mathbf{y}$ es invertible (Teorema 11.6.2). Además tenemos que $\sigma(\mathbf{y} \dot{+} \mathbf{z}) = \sigma \mathbf{y} \dot{+} \sigma \mathbf{z}$ y $\sigma(\mathbf{y} \dot{\times} \mathbf{z}) = \sigma \mathbf{y} \dot{\times} \sigma \mathbf{z}$ pues si $\mathbf{a} = (a_1, \dots, a_n)$ entonces $\sigma \mathbf{a} = (\sigma a_1, \dots, \sigma a_n)$ con $(\sigma \mathbf{a})^{(t)} = \sum_{i=1}^t p^{i-1} (\sigma a_i) p^{t-i} = \sigma(\sum_{i=1}^t p^{i-1} a_i p^{t-i}) = \sigma a^{(t)}$.

El siguiente resultado nos prueba que el primer grupo de cohomología $H^1(W_n(L), G)$ es igual a $\{0\}$. Más precisamente

Teorema 11.7.2. Sea $\varphi: G \rightarrow W_n(L)$ con $\varphi(\sigma) = \mathbf{a}_\sigma$. Si se tiene $\mathbf{a}_\sigma \dot{+} \sigma \mathbf{a}_\tau = \mathbf{a}_{\sigma\tau}$ para cualesquiera $\sigma, \tau \in G$, entonces existe $\mathbf{b} \in W_n(L)$ tal que $\mathbf{a}_\sigma = (1 \dot{-} \sigma) \mathbf{b}$ para toda $\sigma \in G$.

Demostración. Sea $\mathbf{c} = (c_1, \dots, c_n) \in W_n(L)$ tal que $\text{Tr}_{L/K} c_1 \neq 0$. Tal \mathbf{c} existe pues L/K es separable. Ahora por el Teorema 11.6.2, se tiene que $\text{Tr}_{L/K} \mathbf{c} \in W_n(K)$ es invertible. Sea

$$\mathbf{b} := (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \sum_{\tau \in G} \dot{\mathbf{a}}_{\tau} \dot{\times} \tau \mathbf{c}.$$

Entonces, para $\sigma \in G$, se tiene

$$\begin{aligned} (1 \dot{-} \sigma) \mathbf{b} &= \mathbf{b} \dot{-} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \sum_{\tau \in G} \sigma \mathbf{a}_{\tau} \dot{\times} (\sigma \tau) \mathbf{c} \\ &= \mathbf{b} \dot{-} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \left(\sum_{\tau \in G} (\mathbf{a}_{\sigma \tau} \dot{-} \mathbf{a}_{\sigma}) \dot{\times} (\sigma \tau) \mathbf{c} \right) \\ &= \mathbf{b} \dot{-} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \left(\sum_{\tau \in G} \mathbf{a}_{\sigma \tau} \dot{\times} (\sigma \tau) \mathbf{c} \right) \\ &\quad \dot{+} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \mathbf{a}_{\sigma} \dot{\times} \left(\sum_{\tau \in G} (\sigma \tau) \mathbf{c} \right) \\ &= \mathbf{b} \dot{-} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} (\mathrm{Tr}_{L/K} \mathbf{c}) \dot{\times} \mathbf{b} \\ &\quad \dot{+} (\mathrm{Tr}_{L/K} \mathbf{c})^{-1} \dot{\times} \mathbf{a}_{\sigma} \dot{\times} (\mathrm{Tr}_{L/K} \mathbf{c}) \\ &= \mathbf{b} \dot{-} \mathbf{b} \dot{+} \mathbf{a}_{\sigma} = \mathbf{a}_{\sigma} \end{aligned}$$

para toda $\sigma \in G$. □

Definición 11.7.3. Para $\mathbf{y} \in W_n(L)$, se define

$$\wp \mathbf{y} := \mathbf{y}^p \dot{-} \mathbf{y} = (y_1^p, \dots, y_n^p) \dot{-} (y_1, \dots, y_n).$$

Se tiene que $\wp(\mathbf{y} \dot{+} \mathbf{z}) = \wp \mathbf{y} \dot{+} \wp \mathbf{z}$ para cualesquiera $\mathbf{y}, \mathbf{z} \in W_n(L)$.

Proposición 11.7.4. Se tiene que $\wp \mathbf{x} = \mathbf{0} \iff \mathbf{x} \in W_n(\mathbb{F}_p)$.

Demostración. Se tienen las equivalencias

$$\begin{aligned} \wp \mathbf{x} = \mathbf{0} &\iff \mathbf{x}^p = \mathbf{x} \iff (x_1^p, \dots, x_n^p) = (x_1, \dots, x_n) \\ &\iff x_i^p = x_i, 1 \leq i \leq n \iff x_i \in \mathbb{F}_p, 1 \leq i \leq n \iff \mathbf{x} \in W_n(\mathbb{F}_p). \quad \square \end{aligned}$$

Definición 11.7.5. Un vector $\mathbf{x} \in (K)$ se llama *descompuesto* si existe $\mathbf{y} \in W_n(K)$ tal que $\wp \mathbf{y} = \mathbf{x}$. En este caso ponemos $\mathbf{x} \sim \mathbf{0}$, es decir, $\mathbf{x} \sim \mathbf{0}$ es la notación para decir que $\mathbf{x} \in \wp(K)$.

Proposición 11.7.6. Se tiene que $(0, x_2, \dots, x_n) \in W_n(K)$ es descompuesto si y sólo si $(x_2, \dots, x_n) \in W_{n-1}(K)$ es descompuesto.

Demostración. Si $(0, x_2, \dots, x_n) = \wp \mathbf{y} = (\wp y_1, \dots)$ se tiene que $\wp y_1 = 0$ y por tanto $y_1 \in \mathbb{F}_p$. Por tanto $(y_1, 0, \dots, 0) \in W_n(\mathbb{F}_p)$ por lo que $\wp(y_1, 0, \dots, 0) = \mathbf{0}$.

Por otro lado, tenemos de (11.9) se tiene

$$(y_1, y_2, \dots, y_n) = \{y_1\} \dot{+} V(y_2, \dots, y_n) = (y_1, 0, \dots, 0) \dot{+} (0, y_2, \dots, y_n).$$

Por tanto $\wp \mathbf{y} = \wp(\{y_1\}) \dot{+} \wp((0, y_2, \dots, y_n)) = \mathbf{0} \dot{+} \wp((0, y_2, \dots, y_n)) = (0, x_2, \dots, x_n)$. Por lo tanto

$$\wp((y_2, \dots, y_n)) = (x_2, \dots, x_n) \iff \wp((0, y_2, \dots, y_n)) = (0, x_2, \dots, x_n). \quad \square$$

Teorema 11.7.7. *Sea K un campo arbitrario de característica p . Entonces dado $\mathbf{x} \in W_n(K)$, existe $\mathbf{y} \in W_n(\bar{K})$ tal que $\wp \mathbf{y} = \mathbf{x}$ donde \bar{K} denota una cerradura algebraica de K .*

Demostración. Sea $\mathbf{x} = (x_1, x_2, \dots, x_n) \in W_n(K)$. Ahora bien, como $x_1 \in K$ existe $y_1 \in \bar{K}$ tal que $y_1^p - y_1 = x_1$, es decir, $\wp y_1 = x_1$. Se tiene

$$(\wp y_1, x_2, \dots, x_n) = \wp((y_1, 0, \dots, 0)) \dot{+} (0, x'_2, \dots, x'_n).$$

Por inducción en n , existe (y_2, \dots, y_n) tal que $\wp((y_2, \dots, y_n)) = (x'_2, \dots, x'_n)$. Por lo tanto

$$\begin{aligned} \wp(\{y_1\} \dot{+} (0, y_2, \dots, y_n)) &= \wp(y_1, 0, \dots, 0) \dot{+} \wp((0, y_2, \dots, y_n)) \\ &= \wp((y_1, \dots, y_n)) \\ &= (\wp y_1, x_2, \dots, x_n) \dot{+} (0, x'_2, \dots, x'_n) \\ &\quad \dot{+} \wp((0, y_2, \dots, y_n)) \\ &= (\wp y_1, x_2, \dots, x_n) = (x_1, \dots, x_n). \quad \square \end{aligned}$$

Notación 11.7.8. El campo de descomposición de la ecuación $\wp \mathbf{y} = \mathbf{x}$, donde $\mathbf{x} = (x_1, \dots, x_n) \in W_n(K)$, se denota por $K(\mathbf{y}) = K(y_1, \dots, y_n)$ donde $\mathbf{y} = (y_1, \dots, y_n) \in W_n(\bar{K})$. Este campo también se denota por $K(\mathbf{y}) = K(\wp^{-1}\mathbf{x})$.

Proposición 11.7.9. *Sea \mathbf{y}_0 una solución de la ecuación $\wp \mathbf{y} = \mathbf{x}$. Entonces todas las soluciones son $\mathbf{y}_0 \dot{+} \mathbf{m}$ con $m \in \{0, 1, \dots, p^n - 1\}$.*

Demostración. Si $\mathbf{y}, \mathbf{y}' \in W_n(\bar{K})$ son tales que $\wp \mathbf{y} = \wp \mathbf{y}'$, entonces $\wp(\mathbf{y} \dot{-} \mathbf{y}') = \mathbf{0}$ de donde se sigue que $\mathbf{y} \dot{-} \mathbf{y}' \in W_n(\mathbb{F}_p)$. \square

Ahora consideremos K cualquier campo de característica p , $n \in \mathbb{N}$ y $\mathbf{x} = (x_1, \dots, x_n) \in W_n(K)$. Consideremos $\mathbf{y} = (y_1, \dots, y_n)$ solución a la ecuación $\wp \mathbf{y} = \mathbf{x}$ y $L = K(\wp^{-1}\mathbf{x}) = K(\mathbf{y}) = K(y_1, \dots, y_n)$. Puesto que todas las soluciones de la ecuación $\wp \mathbf{y} = \mathbf{x}$ son $\{\mathbf{y}_0 \dot{+} \mathbf{m}\}_{0 \leq m \leq p^n - 1}$ con \mathbf{y}_0 una solución fija, L/K es una extensión normal y separable pues $\mathbf{m} \in W_n(\mathbb{F}_p) \subseteq W_n(K)$. Por lo tanto L/K es una extensión de Galois. Más aún, consideremos la función $\varphi: G := \text{Gal}(L/K) \rightarrow W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z} = C_{p^n}$ dada de la siguiente forma: si $\sigma \in G$, $\sigma \mathbf{y}_0 = \mathbf{y}_0 \dot{+} \mathbf{m}_\sigma$ para algún $m_\sigma \in \{0, 1, \dots, p^n - 1\}$, entonces $\varphi(\sigma) = \mathbf{m}_\sigma$. Se tiene que φ es un monomorfismo de grupos y en particular $G \cong C_{p^t}$ para algún $t \leq n$. Puesto que los subgrupos de C_{p^n} están generados

por \mathbf{p}^i , $0 \leq i \leq n$, se tiene que $G = \langle \sigma_m \rangle$ para algún $0 \leq m \leq n$ donde $\sigma_m(\mathbf{y}_0) = \mathbf{y}_0 \dot{+} \mathbf{p}^m$, $o(G) = p^{n-m}$.

Ahora bien, por el (11.16) se tiene que

$$\begin{aligned}\mathbf{p} &= \mathbf{p} \dot{\times} \mathbf{1} = V(\mathbf{1}^p) = V(\mathbf{1}), \\ \mathbf{p}^2 &= \mathbf{p}^2 \dot{\times} \mathbf{1} = \mathbf{p} \dot{\times} (\mathbf{p} \dot{\times} \mathbf{1}) = \mathbf{p} \dot{\times} V(\mathbf{1}) = V(V(\mathbf{1})^p) = V^2 \mathbf{1},\end{aligned}$$

y en general

$$\mathbf{p}^m = V^m(\mathbf{1}), \quad 0 \leq m \leq n, \quad \mathbf{p}^n = \mathbf{0}.$$

Se tiene

$$\begin{aligned}\sigma_m(\mathbf{y}_0) &= (\sigma_m y_1, \dots, \sigma_m y_n) = \mathbf{y}_0 \dot{+} \mathbf{p}^m = (y_1, \dots, y_n) + V^m(\mathbf{1}) \\ &= (y_1, \dots, y_m, y_{m+1}, \dots, y_n) + \underbrace{(0, 0, \dots, 0, 1, 0, \dots, 0)}_m \\ &= (y_1, \dots, y_m, y'_{m+1}, \dots, y'_n),\end{aligned}$$

por lo que $\sigma_m y_j = y_j$ para $1 \leq j \leq m$ (para $m = 0$ no hay tal que y_j). Esto es, $y_1, \dots, y_m \in K$. En particular $\wp y_1 = x_1 \in \wp(K)$.

En la otra dirección, si $x_1 \notin \wp(K)$, como $\wp \mathbf{y} = \mathbf{x}$, se sigue que $\wp y_1 = x_1$ y por lo tanto $y_1 \notin K$. Observemos que existe $\sigma \in G$ tal que $\sigma y_1 = y_1 + 1$. Digamos que $\sigma(\mathbf{y}_0) = \mathbf{y}_0 \dot{+} \mathbf{m}$, por tanto $\mathbf{m} = (1, \alpha_2, \dots, \alpha_n)$ es invertible en $W_n(\mathbb{F}_p)$. Sea $t \in \mathbb{N}$ tal que $\mathbf{t} \dot{\times} \mathbf{m} = \mathbf{1}$, $\sigma^t(\mathbf{y}_0) = \mathbf{y}_0 \dot{+} \mathbf{t} \dot{\times} \mathbf{m} = \mathbf{y}_0 \dot{+} \mathbf{1}$ y $o(\sigma) = p^n$. En particular $G \cong C_{p^n}$ si y sólo si $x_1 \notin \wp(K)$.

Hemos obtenido

Teorema 11.7.10. *Sea K un campo de característica p , $n \in \mathbb{N}$ y $\mathbf{x} \in W_n(K)$. Entonces la ecuación $\wp \mathbf{y} = \mathbf{x}$ define una extensión de Galois cíclica de K : $L = K(\mathbf{y}) = K(y_1, \dots, y_n) = K(\wp^{-1} \mathbf{x})$. Además $\text{Gal}(L/K) \cong C_{p^{n-m}}$ donde $y_1, \dots, y_m \in K$, $y_{m+1} \notin K$. Finalmente L/K es cíclica de grado p^n si y sólo si $x_1 \notin \wp(K)$ donde $\mathbf{x} = (x_1, \dots, x_n)$. En este último caso, $G = \text{Gal}(L/K)$ está generado por $\sigma(\mathbf{y}) = \mathbf{y} \dot{+} \mathbf{1}$.*

Recíprocamente, si L/K es una extensión cíclica de grado p^n , existe $\mathbf{x} \in W_n(K)$ tal que $L = K(\wp^{-1} \mathbf{x})$, esto es, toda extensión cíclica de grado p^n se obtiene por medio de una ecuación del tipo $\wp \mathbf{y} = \mathbf{x}$.

Demostración. Únicamente falta demostrar que si L/K es cíclica de grado p^n , entonces existe $\mathbf{y} \in W_n(K)$ tal que $L = K(\mathbf{y})$ y donde $\wp \mathbf{y} = \mathbf{x}$.

Sea $G = \text{Gal}(L/K) = \langle \sigma \rangle$, $o(\sigma) = p^n$. Se tiene que $\mathbf{1} \in W_n(L)$ satisface $\text{Tr}_{L/K} \mathbf{1} = \sum_{\sigma \in G} \sigma \mathbf{1} = \mathbf{p}^n \dot{\times} \mathbf{1} = \mathbf{p}^n = \mathbf{0}$. Por el Teorema 11.7.2, existe $\mathbf{y} \in W_n(L)$ tal que $(\sigma \dot{-} \mathbf{1})\mathbf{y} = \mathbf{1}$, esto es, $\sigma \mathbf{y} = \mathbf{y} \dot{+} \mathbf{1}$. Sea $\wp \mathbf{y} = \mathbf{x}$. Entonces

$$\sigma(\wp \mathbf{y}) = \wp(\sigma \mathbf{y}) = \wp(\mathbf{y} \dot{+} \mathbf{1}) = \wp(\mathbf{y}) \dot{+} \wp(\mathbf{1}) = \wp(\mathbf{y}),$$

es decir, $\wp \mathbf{y} = \mathbf{x} \in W_n(K)$. Puesto que $\sigma \mathbf{y} = \mathbf{y} \dot{+} \mathbf{1}$, $K(\mathbf{y}) \subseteq L$ y $K(\mathbf{y})/K$ es una extensión cíclica de orden p^n de donde se sigue que $L = K(\mathbf{y}) = K(\wp^{-1}\mathbf{x})$. \square

Corolario 11.7.11. *Sea $L = K(\mathbf{y}_1) = K(\mathbf{y}_2)$, $\mathbf{y}_1, \mathbf{y}_2 \in W_n(L)$ una extensión cíclica de grado p^n con $\wp \mathbf{y}_i = \mathbf{x}_i \in W_n(K)$, $i = 1, 2$. Entonces existen $\mathbf{j} \in W_n(\mathbb{F}_p)$ invertible y $\mathbf{z} \in W_n(K)$ tal que $\mathbf{y}_1 = \mathbf{j} \dot{\times} \mathbf{y}_2 \dot{+} \mathbf{z}$ y $\mathbf{x}_1 = \mathbf{j} \dot{\times} \mathbf{x}_2 \dot{+} \wp \mathbf{z}$ y recíprocamente.*

Demostración. Sea $G := \text{Gal}(L/K) = \langle \sigma \rangle$ tal que $\sigma \mathbf{y}_1 = \mathbf{y}_1 \dot{+} \mathbf{1}$. Como σ está completamente determinado por $\sigma \mathbf{y}_2$, se tiene que $\sigma \mathbf{y}_2 = \mathbf{y}_2 \dot{+} \mathbf{i}$ con \mathbf{i} invertible en $W_n(\mathbb{F}_p)$ o, equivalentemente, $\text{mcd}(i, p) = 1$. Sea $\mathbf{j} \in W_n(\mathbb{F}_p)$ tal que $\mathbf{j} \dot{\times} \mathbf{i} = \mathbf{1}$. Entonces $\sigma(\mathbf{j} \dot{\times} \mathbf{y}_2) = \mathbf{j} \dot{\times} \mathbf{y}_2 \dot{+} \mathbf{j} \dot{\times} \mathbf{i} = \mathbf{j} \dot{\times} \mathbf{y}_2 \dot{+} \mathbf{1}$. Por tanto $\sigma(\mathbf{y}_1 \dot{-} \mathbf{j} \dot{\times} \mathbf{y}_2) = \mathbf{y}_1 \dot{-} \mathbf{j} \dot{\times} \mathbf{y}_2$ lo cual implica que $\mathbf{y}_1 \dot{-} \mathbf{j} \dot{\times} \mathbf{y}_2 = \mathbf{z} \in W_n(K)$.

El recíproco es claro. \square

Consideramos $L = K(y_1, \dots, y_n)/K$ una extensión cíclica de grado p^n con $\wp \mathbf{y} = \mathbf{x}$. Puesto que $y_n \notin K(y_1, \dots, y_{n-1})$ (pues de lo contrario tendríamos $[L : K] \leq p^{n-1}$), se sigue que $L = K(y_n)$. Ahora bien si $K_{n-1} = K(y_1, \dots, y_{n-1})$, se tiene que

$$\begin{aligned} \wp \mathbf{y} &= \wp \left(\sum_{i=0}^{n-1} V^i(\{y_{i+1}\}) \right) = \wp \left(\sum_{i=0}^{n-2} V^i(\{y_{i+1}\}) \right) \dot{+} \wp(V^{n-1}(\{y_n\})) \\ &= \wp((y_1, \dots, y_{n-1}, 0)) \dot{+} \wp((0, \dots, 0, y_n)) = \mathbf{x}, \end{aligned}$$

$\wp((0, \dots, 0, y_n)) = (0, \dots, 0, y_n^p - y_n)$. Por tanto, tomando la componente fantasma n , si sigue que $y_n^p - y_n = z_{n-1} + x_n$ con $z_{n-1} \in K_{n-1}$.

Por el Teorema 11.2.4 se tiene que si $\langle \sigma \rangle = \text{Gal}(L/K)$, $\varphi|_{K_{n-1}}$, entonces $\wp y_n = y_n^p - y_n = z_{n-1} + x_n$, $(\sigma - 1)y_n = \delta$ con $(\varphi - 1)z_{n-1} = \wp \delta$. Con esto recuperamos el resultado de Schmid (11.1) para la generación de una extensión cíclica de grado p^n .

Teorema 11.7.12. *Sea L/K una extensión cíclica de grado p^n y sean $K_0 = K \subseteq K_1 \subseteq \dots \subseteq K_{n-1} \subseteq K_n = L$ tales que $[K_i : K] = p^i$ y sea $\langle \sigma_i \rangle = \text{Gal}(K_i/K)$, $K_i = K_{i-1}(y_i)$. Se tiene $\sigma_i = \sigma_n|_{K_i}$. Entonces L/K satisface*

$$\begin{aligned} K_1 &= K(y_1), & \wp y_1 &= x_1, & (\sigma_1 - 1)y_1 &= 1, \\ K_2 &= K_1(y_2), & \wp y_2 &= z_1 + x_2, & (\sigma_2 - 1)y_2 &= c_1, & (\sigma_1 - 1)z_1 &= \wp c_1 \\ K_3 &= K_2(y_3), & \wp y_3 &= z_2 + x_3, & (\sigma_3 - 1)y_3 &= c_2, & (\sigma_2 - 1)z_2 &= \wp c_2 \\ &\vdots & \vdots & & \vdots & & \vdots \\ L = K_n &= K_{n-1}(y_n), & \wp y_n &= z_{n-1} + x_n, & (\sigma_n - 1)y_n &= c_{n-1}, & (\sigma_{n-1} - 1)z_{n-1} &= \wp c_{n-1} \end{aligned} \quad (11.19)$$

donde $z_i, c_i \in K_i$, $1 \leq i \leq n-1$, $y_i \in K_i$ ($y_i \notin K_{i-1}$) y $x_1, \dots, x_n \in K$ con $x_1 \notin \wp(K)$. Toda extensión cíclica de grado p^n está determinado por elementos arbitrarios $x_1, \dots, x_n \in K$ con $x_1 \notin \wp(K)$. \square

11.8. Sobre el conductor

Primero se define el *conductor* para campos locales. Un *campo local* es un campo completo bajo una valuación no arquimediana con campo residual finito.

Sea K un campo completo con respecto a una valuación discreta v y el cual tiene campo residual finito. Sea L/K una extensión abeliana finita. Sea n el mínimo $n \in \mathbb{N} \cup \{0\}$ tal que $U_K^{(n)} \subseteq N_{L/K}L^*$ donde \mathfrak{p} es el ideal primo del anillo de enteros $\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}$, es decir, $\mathfrak{p} = \{x \in K \mid v(x) > 0\}$ y $U^{(n)} := 1 + \mathfrak{p}^n$.

Por teoría de campos de clase, [51, Theorem 1.4, p. 321] se tiene que $N_{L/K}L^*$ es abierto en K^* y $1 \in N_{L/K}L^*$ por lo que tal n existe por ser $\{U_K^{(n)}\}_{n=0}^\infty$ un sistema fundamental de vecindades abiertas de 1.

Definición 11.8.1. Se define el *conductor* de L/K por

$$\mathfrak{f} = \mathfrak{f}_K = \mathfrak{f}(L/K) := \mathfrak{p}^n.$$

Se tiene que una extensión abeliana de campos locales L/K es no ramificada si y sólo si su conductor es $\mathfrak{f} = 1$ ([51, Proposition 1.7, p. 323]).

Teorema 11.8.2 ([51, Theorem 1.4, p. 321]). Sea K un campo local. El mapeo

$$L \mapsto \mathcal{N}_L := N_{L/K}L^*$$

establece una correspondencia uno a uno entre las extensiones abelianas finitas L/K y los subgrupos abiertos de índice finito en K^* . Más aún:

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}. \quad \square$$

Ahora, en *campos globales*, es decir, extensiones finitas de \mathbb{Q} o de $\mathbb{F}_p(t)$ se usan los conceptos de *adèles* y de *idéles*. Sea K un campo global. Un *adèle* o *idéle aditivo* o *repartición* es una familia $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$ con $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}$, la completación de K en \mathfrak{p} y además $\alpha_{\mathfrak{p}}$ es entero para casi todo \mathfrak{p} , esto es, $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \geq 0$ para casi todo \mathfrak{p} y donde \mathfrak{p} recorre todos los divisores primos de K , incluyendo los primos infinitos.

Se denota $\mathbb{A}_K := \prod'_{\mathfrak{p}} K_{\mathfrak{p}}$ (producto restringido) el *anillo de los adèles* con suma y multiplicación por componentes. El grupo de *idéles* de K se define como el grupo de las unidades de \mathbb{A}_K^* , es decir, $\mathbb{I}_K = \mathbb{A}_K^*$. Esto es, un idéle es una familia $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$, $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$ y $\alpha_{\mathfrak{p}}$ es una unidad en el anillo de enteros $\mathcal{O}_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$ para casi toda \mathfrak{p} . Se escribe $\mathbb{I}_K = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}^*$. De manera natural $K^* \subseteq \mathbb{I}_K$ vía el mapeo diagonal, K^* son los *idéles principales*. Sea $C_K := \mathbb{I}_K / K^*$. El grupo C_K recibe el nombre de el *grupo de clases de idéles*.

Proposición 11.8.3. Si Cl_K denota el grupo de clases de K , y $\mathbb{I}_K^{S_\infty} = \prod_{\mathfrak{p} \mid \infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}}$, entonces $Cl_K \cong \mathbb{I}_K / \mathbb{I}_K^{S_\infty} K^* \cong C_K / ((\mathbb{I}_K^{S_\infty} K^*) / K^*)$ ([51, Proposition 1.3, p. 360]). \square

Un *módulo* es un ideal entero $\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{n_{\mathfrak{p}}}$ de \mathcal{O}_K , el anillo de enteros de K al cual lo consideramos como $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ con $n_{\mathfrak{p}} = 0$ para $\mathfrak{p} \mid \infty$. Se define para cada lugar \mathfrak{p} de K :

$$U_{\mathfrak{p}}^{(0)} = U_{\mathfrak{p}} \quad \text{y} \quad U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} = \begin{cases} 1 + \mathfrak{p}^{n_{\mathfrak{p}}} & \text{si } \mathfrak{p} \nmid \infty, \\ \mathbb{R}_+^* \subseteq K_{\mathfrak{p}}^* & \text{si } \mathfrak{p} \text{ es real,} \\ \mathbb{C}^* = K_{\mathfrak{p}}^* & \text{si } \mathfrak{p} \text{ es complejo,} \end{cases}$$

para $n_{\mathfrak{p}} > 0$. Se define $\alpha_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}^{n_{\mathfrak{p}}}} \iff \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$. Esta definición corresponde a la congruencia usual si \mathfrak{p} es finito, $\alpha_{\mathfrak{p}} > 0$ si \mathfrak{p} es real y es una condición vacía para \mathfrak{p} complejo.

Definición 11.8.4 ([51, 1.7, p. 363]). Se define $C_K^{\mathfrak{m}} := \mathbb{I}_K^{\mathfrak{m}} K^* / K^*$ donde $\mathbb{I}_K^{\mathfrak{m}} := \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$. El grupo $C_K^{\mathfrak{m}}$ recibe el nombre de *grupo de congruencia módulo \mathfrak{m}* . Al grupo $C_K / C_K^{\mathfrak{m}}$ se le llama el *grupo de rayos módulo \mathfrak{m}* .

Si L/K es una extensión de Galois, hay una norma $N_{L/K} : \mathbb{I}_L \rightarrow \mathbb{I}_K$ definida como sigue ([51, p. 370]). Sea \mathfrak{p} un lugar de K y sea $L_{\mathfrak{p}} := \prod_{\mathfrak{P} \mid \mathfrak{p}} L_{\mathfrak{P}}$. Cada $\alpha_{\mathfrak{p}} \in L_{\mathfrak{p}}^*$ define un automorfismo $\alpha_{\mathfrak{p}} : L_{\mathfrak{p}} \rightarrow L_{\mathfrak{p}}$, $x \mapsto \alpha_{\mathfrak{p}} x$ del $K_{\mathfrak{p}}$ -espacio vectorial $L_{\mathfrak{p}}$. Se define la norma de $\alpha_{\mathfrak{p}}$ por: $N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}) = \text{gr}(\alpha_{\mathfrak{p}})$. Se induce un homomorfismo $N_{L/K} : \mathbb{I}_L \rightarrow \mathbb{I}_K$ dado por: si $\alpha = (\alpha_{\mathfrak{P}}) \in \mathbb{I}_L$, las componentes locales de $N_{L/K}(\alpha)$ están dadas por ([51, Proposition 2.2, p. 370])

$$N_{L/K}(\alpha)_{\mathfrak{p}} = \prod_{\mathfrak{P} \mid \mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}).$$

Ahora $N_{L/K}$ manda idéles principales en idéles principales y por tanto la norma induce otra norma $N_{L/K} : C_L \rightarrow C_K$ ([51, p. 370]). Se tiene

Teorema 11.8.5 ([51, Theorem 6.1, p. 395]). Sea K un campo global. El mapeo

$$L \mapsto \mathcal{N}_L := N_{L/K} C_L$$

es una correspondencia uno a uno entre las extensiones abelianas finitas L/K y los subgrupos cerrados de índice finito en C_K . Más aún:

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}.$$

El campo L/K que corresponde al subgrupo \mathcal{N} de C_K se llama el campo de clase de \mathcal{N} . Se tiene

$$\text{Gal}(L/K) \cong C_K / \mathcal{N}. \quad \square$$

Ahora bien, entre los grupos cerrados de C_K de índice finito están los grupos de congruencias $C_K^{\mathfrak{m}}$ donde $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$.

Definición 11.8.6 ([51, 6.2, p. 396]). El campo de clase $K^{\mathfrak{m}}/K$ que corresponde a $C_K^{\mathfrak{m}}$ se llama el *campo de clases de rayos módulo \mathfrak{m}* .

Se tiene $\text{Gal}(K^{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}$ y si $\mathfrak{m} \mid \mathfrak{m}'$ entonces $K^{\mathfrak{m}} \subseteq K^{\mathfrak{m}'}$ ([51, p. 396–397]). Ahora bien si \mathcal{N} es cualquier grupo cerrado de índice finito en C_K , \mathcal{N} contiene a un subgrupo de congruencia $C_K^{\mathfrak{m}}$ y por tanto toda extensión abeliana L/K está contenida en un campo de clase $K^{\mathfrak{m}}/K$.

Definición 11.8.7 ([51, 6.4, p. 397]). Sea L/K una extensión abeliana finita. Sea $\mathcal{N}_L = N_{L/K}C_L$. Se define el *conductor* $\mathfrak{f}(L/K) = \mathfrak{f}$ de L/K como el máximo común divisor de los módulos \mathfrak{m} tales que $L \subseteq K^{\mathfrak{m}}$: $\mathfrak{f} := \text{mcd}\{\mathfrak{m} \mid \mathfrak{m} \text{ es un módulo y } L \subseteq K^{\mathfrak{m}}\}$. Esto es, $\mathfrak{f} = \text{mcd}\{\mathfrak{m} \mid \mathfrak{m} \text{ es un módulo y } C_K^{\mathfrak{m}} \subseteq \mathcal{N}_L\}$.

En otras palabras $K^{\mathfrak{f}}/K$ es el mínimo campo de clases de rayos que contiene a L/K . Una observación interesante es que \mathfrak{m} no necesariamente es el conductor de $K^{\mathfrak{m}}/K$, es decir, puede existir $\mathfrak{f} \mid \mathfrak{m}$, $\mathfrak{f} \neq \mathfrak{m}$ y $K^{\mathfrak{f}} = K^{\mathfrak{m}}$ (o $C_K^{\mathfrak{m}} = C_K^{\mathfrak{f}}$).

La relación entre los conductores locales y los conductores globales es:

Teorema 11.8.8 ([51, Proposition 6.5, p. 397]). Si \mathfrak{f} es el conductor de una extensión abeliana finita L/K de campos globales y $\mathfrak{f}_{\mathfrak{p}}$ es el conductor de la extensión local $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ ($L_{\mathfrak{p}}$ una extensión de $K_{\mathfrak{p}}$, es decir, si $\mathfrak{P}_1, \dots, \mathfrak{P}_r \mid \mathfrak{p}$, escogemos cualquier $\mathfrak{P}_i \mid \mathfrak{p}$ y ponemos $L_{\mathfrak{p}} := L_{\mathfrak{P}_i}$), entonces si definimos $\mathfrak{f}_{\mathfrak{p}} = 1$ para \mathfrak{p} infinito, se tiene

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}}. \quad \square$$

Corolario 11.8.9 ([51, 6.6, p. 398]). Dada una extensión abeliana finita de campos globales L/K , se tiene que \mathfrak{p} se ramifica en L si y sólo si $\mathfrak{p} \mid \mathfrak{f}$. \square

Ejemplo 11.8.10 ([51, 6.7, p. 398]). Los campos de clases de rayos de \mathbb{Q} son precisamente los campos ciclotómicos pues los módulos están dados por $\mathfrak{m} = (m)$, $m \in \mathbb{N}$ y $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$ y en particular toda extensión abeliana de \mathbb{Q} está contenida en un campo ciclotómico. Se sigue de esto una prueba del Teorema de Kronecker–Weber para campos numéricos: la máxima extensión abeliana de \mathbb{Q} es $\mathbb{Q}^{ab} = \cup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$.

Observación 11.8.11. Vemos que dado un campo numérico K , los campos $K^{\mathfrak{m}}$ son los análogos a los campos $\mathbb{Q}(\zeta_m)$, pues cada extensión abeliana de K está contenida en algún $K^{\mathfrak{m}}$ y cada extensión abeliana de \mathbb{Q} está contenida en algún $\mathbb{Q}(\zeta_m)$. Ahora bien, la gran diferencia es que sabemos la existencia de los campos $K^{\mathfrak{m}}$ pero no como están generados, a diferencia de los campos ciclotómicos $\mathbb{Q}(\zeta_m)$ que explícitamente están dados por las raíces de la ecuación $x^m - 1$.

Observación 11.8.12. Dado un campo numérico K , el campo de clase K^1 corresponde a la máxima extensión abeliana de K no ramificada en ningún primo finito. Este campo es usualmente llamado el *campo grande de clases de Hilbert*. Los primos infinitos pueden o no ser ramificados en K^1/K . Notemos que $\mathbb{Q}^1 = \mathbb{Q}$.

Definición 11.8.13. El subcampo $K \subseteq K_H \subseteq K^1$ tal que los primos infinitos de K son no ramificados o, equivalentemente, se descomponen totalmente, se llama *el campo de clases de Hilbert*.

Teorema 11.8.14 (Campo de clase de Hilbert, [51, Proposition 6.8, p. 399]). *Se tiene que el grupo de Galois de K_H/K satisface $\text{Gal}(K_H/K) \cong \text{Cl}_K$, el grupo de clases de K .* \square

11.8.1. Representaciones, caracteres y conductores

Definición 11.8.15. Una *representación* de un grupo finito G es una acción de G en un \mathbb{C} -espacio vectorial de dimensión finita V . Equivalentemente, una representación es un homomorfismo de grupos

$$\rho: G \rightarrow \text{GL}(V) = \text{Aut}_{\mathbb{C}}(V).$$

Una acción la podemos entender como: $\varphi: G \times V \rightarrow V$ con $\varphi(\sigma, v) := \sigma \circ v := \rho(\sigma)(v)$. También es común usar la notación (V, ρ) para indicar la representación de G en V .

La *representación trivial* es (ρ, \mathbb{C}) con $\rho(\sigma) = 1$ para toda $\sigma \in G$. El *grado* de la representación es la dimensión de V .

Una representación ρ se llama *irreducible* si V no admite ningún subespacio propio $0 \subsetneq W \subsetneq V$ que sea G -invariante, es decir, $\sigma \circ W \subseteq W$ para toda $\sigma \in G$.

Proposición 11.8.16. *Si G es abeliano, toda representación irreducible de G es de grado 1, es decir es un caracter*

$$\rho: G \rightarrow \text{GL}_1(\mathbb{C}) \cong \mathbb{C}^*. \quad \square$$

Se tiene que toda representación (ρ, V) se factoriza a través de una suma directa $V = V_1 \oplus \cdots \oplus V_s$ de representaciones irreducibles. Más precisamente, $\rho_i: G \rightarrow \text{GL}(V_i)$ es una representación irreducible y $\rho = \rho_1 \oplus \cdots \oplus \rho_s$. Explícitamente si $\{v_{ij}\}_{j=1}^{m_i}$ es una base de V_i y consideramos la base de V dada por $\{v_{ij}\}_{1 \leq j \leq m_i, 1 \leq i \leq s}$ y si la matriz de $\rho_i(\sigma)$ con respecto a la base $\{v_{ij}\}_{j=1}^{m_i}$ es la matriz $(m_i \times m_i)$ $A_{\sigma,i}$, entonces $\rho(\sigma)$ es la matriz

$$A_{\sigma} = \begin{pmatrix} \boxed{A_{\sigma,1}} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_{\sigma,s}} \end{pmatrix}$$

con respecto a la base $\{v_{ij}\}_{1 \leq i \leq s}^{1 \leq j \leq m_i}$.

Dos representaciones (ρ, \bar{V}) y (ρ', V') se llaman *equivalentes* si existe un isomorfismo $\varphi: V \rightarrow V'$ de G -espacios vectoriales, esto es, φ es un isomorfismo de espacios vectoriales tal que $\varphi(\sigma \circ v) = \sigma \circ \varphi(v)$ para toda $\sigma \in G$ y toda $v \in V$.

Si en la suma de G -espacios $V = V_1 \oplus \cdots \oplus V_s$ una representación (ρ_α, V_α) tiene r_α representaciones equivalentes entre las representaciones $(\rho_1, V_1), \dots, (\rho_s, V_s)$, se usa la notación:

$$\rho \sim \sum_{\alpha} r_{\alpha} \rho_{\alpha}$$

y r_{α} se llama la *multiplicidad* de ρ_{α} en ρ .

Definición 11.8.17. Dada una representación (ρ, V) el *caracter* de ρ se define por

$$\chi_{\rho}: G \rightarrow \mathbb{C}, \quad \chi_{\rho}(\sigma) = \text{traza de } \rho(\sigma).$$

Se tiene que si $\rho \sim \sum_{\alpha} r_{\alpha} \rho_{\alpha}$, entonces $\chi_{\rho} = \sum_{\alpha} r_{\alpha} \chi_{\rho_{\alpha}}$.

Un caracter χ se llama *irreducible* si χ es el caracter de una representación irreducible. Una *función central* o *función de clase* es una función $f: G \rightarrow \mathbb{C}$ tal que $f(\sigma\tau\sigma^{-1}) = f(\tau)$ para cualesquiera $\sigma, \tau \in G$.

Teorema 11.8.18. *Se tiene que dos representaciones son equivalentes si y sólo si sus caracteres son iguales.* \square

Se tiene que toda función central φ se puede escribir unívocamente como una combinación lineal

$$\varphi = \sum_{\chi} c_{\chi} \chi, \quad c_{\chi} \in \mathbb{C},$$

donde los χ 's son caracteres irreducibles.

Teorema 11.8.19. *Se tiene que φ es el caracter de una representación si y sólo si $c_{\chi} \in \mathbb{N} \cup \{0\}$ para toda χ .* \square

Se tiene que si (ρ, V) es una representación con caracter χ , se tiene $\dim V^G = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)$.

11.8.2. Conductores de Artin

Sea L/K una extensión de Galois de campos globales. Sea $G = \text{Gal}(L/K)$. Dado un caracter irreducible χ de G , se define el ideal $\mathfrak{f}(\chi)$ por:

$$\mathfrak{f}(\chi) := \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{f_{\mathfrak{p}}(\chi)} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{f}_{\mathfrak{p}}(\chi)$$

con

$$f_{\mathfrak{p}}(\chi) = \sum_{i \geq 0} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}$$

donde V es una representación con caracter χ , G_i es el i -ésimo grupo de ramificación de $L_{\mathfrak{p}}/K_{\mathfrak{p}}$, y g_i es el orden de G_i donde \mathfrak{P} es cualquier divisor en L dividiendo a \mathfrak{p} .

Definición 11.8.20. Al ideal $\mathfrak{f}(\chi)$ se le llama el *conductor de Artin* del caracter χ .

Para campos locales, $\mathfrak{f}_{\mathfrak{p}}(\chi) = \mathfrak{p}^{f(\chi)}$ se define como el *conductor local de Artin* del caracter χ .

En realidad el conductor local de Artin se define de manera más general como sigue. Sea L/K una extensión de campos locales, con grupo de Galois $G = \operatorname{Gal}(L/K)$. Sea f el grado de inercia de L/K . Se define $i_G(\sigma) = v_L(\sigma x - x)$ donde x es cualquier elemento tal que $\mathcal{O}_L = \mathcal{O}_K[x]$ y v_L es la valuación de L . Sea

$$a_G(\sigma) = \begin{cases} -f i_G(\sigma) & \text{para } \sigma \neq 1, \\ f \sum_{\tau \neq 1} i_G(\tau) & \text{para } \sigma = 1. \end{cases}$$

Se tiene que a_G es una función central sobre G y se puede escribir

$$a_G = \sum_{\chi} f(\chi) \chi, \quad f(\chi) \in \mathbb{C},$$

donde χ varía sobre los caracteres irreducibles de G . Se tiene que $f(\chi)$ es un entero no negativo y por lo tanto podemos formar el ideal $\mathfrak{f}_{\mathfrak{p}}(\chi) = \mathfrak{p}^{f(\chi)}$, que será la \mathfrak{p} -componente del conductor de Artin global.

La relación entre los conductores de Artin y los conductores local y global antes definidos, se obtiene de los siguientes resultados.

Teorema 11.8.21 ([51, Proposition 11.6, p. 532]). *Sea L/K una extensión de Galois de campos locales y sea χ un caracter de $\operatorname{Gal}(L/K)$ de grado 1. Sea $L_{\chi} = L^{\operatorname{nuc} \chi}$ el campo fijo del núcleo de χ . Sea \mathfrak{f} el conductor de L_{χ}/K . Entonces*

$$\mathfrak{f} = \mathfrak{f}_{\mathfrak{p}}(\chi). \quad \square$$

En el caso global tenemos:

Teorema 11.8.22 ([51, Proposition 11.10, p. 535]). *Sea L/K una extensión de campos globales, χ un caracter de $\operatorname{Gal}(L/K)$ de grado 1. Sea L_{χ} el campo fijo de $\operatorname{nuc} \chi$ y sea \mathfrak{f}_{χ} el conductor global de la extensión L_{χ}/K . Entonces*

$$\mathfrak{f}_{\chi} = \mathfrak{f}(\chi). \quad \square$$

Como consecuencia, puesto que una extensión abeliana L/K , ya sea de campos locales o globales, se tiene que los conductores de Artin y los conductores usuales con lo mismo. Así, en el caso abeliano, los conductores se pueden considerar, en caso de así convenir, como conductores de Artin. Por otro lado se tiene la siguiente fórmula hallada por H. Hasse y E. Artin.

Teorema 11.8.23 (Fórmula del conductor–discriminante, [51, 11.9, p. 534]). *Para cualquier extensión finita de Galois L/K de campos globales, se tiene*

$$\mathfrak{d}_{L/K} = \prod_{\chi} \mathfrak{f}(\chi)^{\chi(1)}$$

donde χ recorre el conjunto de todos los caracteres irreducibles de $\text{Gal}(L/K)$ y $\mathfrak{d}_{L/K}$ denota el discriminante de la extensión L/K . \square

Notemos que $\chi(1)$ es precisamente la dimensión de la representación asociada a χ .

En lo que resta de este capítulo el campo de funciones racionales sobre \mathbb{F}_q será denotado por K : $K = \mathbb{F}_q(T)$. Como es usual R_T denota el anillo de polinomios en T sobre \mathbb{F}_q : $R_T = \mathbb{F}_q[T]$.

Sea ahora $\chi: (R_T/(M))^* \rightarrow \mathbb{C}^*$ un caracter de Dirichlet. Se tiene que si \mathfrak{f}_χ es el conductor de χ (como caracter de Dirichlet) y si \mathfrak{f}'_χ es el conductor de Artin de χ , entonces $\mathfrak{f}_\chi = \mathfrak{f}'_\chi$. Por otro lado el conductor de Dirichlet de un caracter χ es P^α con $P \in R_T$ es mónico e irreducible, si y sólo si $\chi: (R_T/(P^\alpha))^* \rightarrow \mathbb{C}^*$ pero no puede definirse módulo $P^{\alpha-1}$: $\chi: (R_T/(P^{\alpha-1}))^* \rightarrow \mathbb{C}^*$.

11.8.3. Conductor local de $K(\Lambda_{P^\alpha})$

Se tiene que $K(\Lambda_{P^\alpha})_{\mathfrak{B}} \cong \mathbb{F}_q((\lambda_{P^\alpha}))$ pues P es totalmente ramificado y $v_{\mathfrak{B}}(\lambda_{P^\alpha}) = 1$, donde $\lambda = \lambda_{P^\alpha}$ es generador de Λ_{P^α} y \mathfrak{B} es el primo en $K(\Lambda_{P^\alpha})$ sobre P . Ahora se tiene que $N_{K(\Lambda_{P^\alpha})_{\mathfrak{B}}/K_P}(K(\Lambda_{P^\alpha})_{\mathfrak{B}}^*) = (P) \times U_P^{(\alpha)}$ ([51, Proposition 1.8, Capítulo V, p. 323]).

Como consecuencia, se tiene que el conductor local de $K(\Lambda_{P^\alpha})/K$ en P es P^α y 1 para cualquier otro $Q \neq P$, $Q \in R_T$ irreducible.

Lema 11.8.24. *Supongamos que $\mathcal{K} \subseteq K(\Lambda_{P^\beta})$ para algún β y sea $\mathfrak{f}_{\mathcal{K}} = P^\gamma$. Entonces $\gamma \leq \alpha \iff \mathcal{K} \subseteq K(\Lambda_{P^\alpha})$.*

Demostración.

\implies .- Supongamos que $\mathcal{K} \not\subseteq K(\Lambda_{P^\alpha})$ y sea $L = \mathcal{K}K(\Lambda_{P^\alpha}) \not\subseteq K(\Lambda_{P^\alpha})$. Entonces por el Teorema 11.8.2 se tiene que $\mathcal{N}_L \subsetneq \mathcal{N}_{K(\Lambda_{P^\alpha})} = (P) \times U^{(\alpha)}$. Sea $\mathfrak{f}_L = P^\delta$. Entonces $U^{(\delta)} \subseteq \mathcal{N}_L$ y $U^{(\delta-1)} \not\subseteq \mathcal{N}_L$. Además $P \in \mathcal{N}_L$ lo cual implica que

$$(P) \times U^{(\delta)} \subseteq \mathcal{N}_L \subsetneq \mathcal{N}_{K(\Lambda_{P^\alpha})} = (P) \times U^{(\alpha)},$$

de donde se sigue que $\delta > \alpha$. Ahora bien se tiene que

$$\mathfrak{f}_L = \mathfrak{f}_{\mathcal{K}K(\Lambda_{P^\alpha})} = \mathfrak{f}^{\max\{\gamma, \alpha\}} = P^\gamma = P^\delta$$

por lo que obtenemos $\delta = \gamma > \alpha$. Este absurdo prueba que $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$.

\Leftarrow .- Se tiene que $U^{(\alpha)} \subseteq \mathcal{N}_{K(\Lambda_{P^\alpha})} \subseteq \mathcal{N}_{\mathcal{K}}$, de donde se sigue $\alpha \geq \gamma$. \square

Como consecuencia tenemos

Proposición 11.8.25. *Sea $\mathcal{K} \subseteq K(\Lambda_{P^\beta})$ para algún $\beta \in \mathbb{N}$. Entonces $\mathfrak{f}_{\mathcal{K}} = P^\alpha$ si y sólo si $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ y $\mathcal{K} \not\subseteq K(\Lambda_{P^{\alpha-1}})$.*

Demostración. Si $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ y $\mathcal{K} \not\subseteq K(\Lambda_{P^{\alpha-1}})$ entonces si $\mathfrak{f}_{\mathcal{K}} = P^\gamma$ se sigue del Lema 11.8.24 que $\gamma \leq \alpha$ y $\gamma \not\leq \alpha - 1$ por lo que $\gamma = \alpha$.

Recíprocamente, si $\mathfrak{f}_{\mathcal{K}} = P^\alpha$ entonces nuevamente por el Lema 11.8.24, y puesto que $\alpha \leq \alpha$ se sigue que $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$. Ahora bien, si tuviésemos $\mathcal{K} \subseteq K(\Lambda_{P^{\alpha-1}})$ entonces se seguiría que $\alpha \leq \alpha - 1$ lo que prueba que $\mathcal{K} \not\subseteq K(\Lambda_{P^{\alpha-1}})$. \square

11.8.4. El conductor de acuerdo a Schmid

Nuestro objetivo en esta subsección es enunciar el cálculo de Schmid para el conductor en una extensión cíclica determinada por un vector de Witt.

Proposición 11.8.26. *Sea \mathcal{K}/K una extensión cíclica de grado p tal que $\mathcal{K} \subseteq K(\Lambda_{P^\beta})$ para algún $\beta \in \mathbb{N}$. Entonces existe $y \in \mathcal{K}$ tal que $\mathcal{K} = K(y)$ con $\wp y = y^p - y = h(T) \in K$ con $h(T) = \frac{g(T)}{P(T)^\lambda}$ con $g(T) \in R_T$, $\text{mcd}(P(T), g(T)) = 1$, $\lambda > 0$ y $\text{mcd}(\lambda, p) = 1$.*

Demostración. Por el Teorema 11.2.1 se tiene que existe $y \in \mathcal{K}$ tal que $\mathcal{K} = K(y)$ y $y^p - y = h(T) \in K$. Se tiene $\mu(X) = \text{Irr}(y, X, K) = X^p - X - h(T)$ con $h(T) \in K$ y $h(T) \notin \wp(K) = \{a^p - a \mid a \in K\}$. Sea $h(T) = \frac{g(T)}{f(T)}$ con $g(T), f(T) \in R_T$, $\text{mcd}(g(T), f(T)) = 1$, $f(T) = \prod_{i=1}^r P_i^{\alpha_i}$, donde P_1, \dots, P_r son polinomios irreducibles distintos. Descomponiendo a $h(T)$ en fracciones parciales, se tiene

$$\frac{g(T)}{f(T)} = s(T) + \sum_{i=1}^r \frac{t_i(T)}{P_i(T)^{\alpha_i}}, \quad \text{gr } t_i(T) < \text{gr } P_i(T)^{\alpha_i}, \quad t_i(T), s(T) \in R_T.$$

Se tiene que para cualquier divisor primo $\mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{p}_\infty\}$, donde \mathfrak{p}_i denota al divisor primo correspondiente a P_i , se tiene $v_{\mathfrak{p}}(y^p - y) = v_{\mathfrak{p}}(h) \geq 0$. Es decir, y es entero con respecto a \mathfrak{p} . Se sigue que

$$\mu(X) = \prod_{i=0}^{p-1} (X - y - i) \quad \text{y} \quad \mu'(X) = \sum_{i=0}^{p-1} \prod_{j \neq i} (X - y - i).$$

Por lo tanto $\mu'(y) = \sum_{i=0}^{p-1} \prod_{j \neq i} (y - y - j) = \prod_{j=1}^{p-1} (-j)$ es una unidad y por el Teorema 8.5.6, \mathfrak{p} es no ramificado.

Ahora si para algún $1 \leq i \leq r$, $p \mid \alpha_i$ entonces si $\alpha_i = \lambda_i p$, podemos escribir

$$\frac{g(T)}{f(T)} = \frac{t_0(T)}{P_i(T)^{\lambda_i p}} + s_i(T) \quad \text{con} \quad v_{\mathfrak{p}_i}(s_i(T)) \geq 0, \quad \text{gr } t_0(T) < \text{gr } P_i(T)^{\lambda_i p}.$$

Ahora $K(T)/(P_i(T))$ es un campo finito, por lo tanto perfecto. Existe $m(T) \in K(T)$ tal que $m(T)^p \equiv t_0(T) \pmod{P_i(T)}$. Sea $n(T) := -\frac{m(T)}{P_i(T)^{\lambda_i}}$. Sea $u = y + n(T)$. Entonces $\mathcal{K} = K(u) = K(y)$ y

$$u^p - u = h(T) + n(T)^p - n(T) = h_0(T)$$

con $v_{\mathfrak{p}_i}(h_0(T)) > -\lambda_i p$, $v_{\mathfrak{p}_j}(h_0(T)) = v_{\mathfrak{p}_j}(h(T))$ para $j \neq i$ y $v_{\mathfrak{p}}(h(T)) \geq 0$ para $\mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{p}_\infty\}$. Continuando con este proceso, se obtiene $\mathcal{K} = K(w)$ con $w^p - w = \ell(T)$ con $(\ell(T))_K = \frac{\mathfrak{C}}{\mathfrak{p}_1^{\lambda_1} \dots \mathfrak{p}_m^{\lambda_m}} \mathfrak{p}_\infty^s$ con \mathfrak{C} un divisor entero primo relativo a $\mathfrak{p}_1, \dots, \mathfrak{p}_m$, $m \leq r$, $\lambda_i > 0$, $\text{mcd}(\lambda_i, p) = 1$ donde reenumeramos a los elementos de $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ del conjunto inicial en caso de ser necesario.

Para $1 \leq i \leq m$ se tiene $v_{\mathfrak{p}_i}(w^p - w) = v_{\mathfrak{p}_i}(\ell(T)) = e(\mathfrak{P}_i \mid \mathfrak{p}) v_{\mathfrak{p}_i}(\ell(T)) = -e(\mathfrak{P}_i \mid \mathfrak{p}) \lambda_i < 0$, donde \mathfrak{P}_i es un divisor en \mathcal{K} sobre \mathfrak{p}_i . Por tanto $v_{\mathfrak{p}_i}(w) < 0$ y $v_{\mathfrak{p}_i}(w^p - w) = v_{\mathfrak{p}_i}(w^p) = p v_{\mathfrak{p}_i}(w) = -e(\mathfrak{P}_i \mid \mathfrak{p}) \lambda_i$. Puesto que $\text{mcd}(p, \lambda_i) = 1$, se tiene que $p \mid e(\mathfrak{P}_i \mid \mathfrak{p})$ y por tanto \mathfrak{p}_i es ramificado en \mathcal{K}/K . Por otro lado, como $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$, el único primo finito ramificado es \mathfrak{p} , el divisor asociado a P y por tanto se tiene $\mathcal{K} = K(y)$ con

$$y^p - y = \frac{g(T)}{P(T)^\lambda} \quad \text{con} \quad g(T) \in R_T, \quad \text{mcd}(g(T), P(T)) = 1, \\ \lambda > 0 \quad \text{y} \quad \text{mcd}(\lambda, p) = 1. \quad \square$$

Corolario 11.8.27. Si \mathcal{K}/K es una extensión cíclica de grado p^n con $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$, entonces existe \mathbf{y} tal que $\mathcal{K} = K(\mathbf{y})$ con $\mathbf{y}^p = \mathbf{\beta}$ y $\mathbf{\beta} = \beta \in W_n(K)$ con $\beta_i(T) = \frac{g_i(T)}{P(T)^{\lambda_i}}$ con $g_i(T) \in R_T$, $\lambda_i \geq 0$ y si $\lambda_i > 0$ entonces $\text{mcd}(g_i(T), P(T)) = 1$ y $\text{mcd}(\lambda_i, p) = 1$. Finalmente, $\lambda_1 > 0$.

Demostración. Procedemos por inducción en n . El caso $n = 1$ es la Proposición 11.8.26. Para el caso $n + 1$, $\mathcal{K}_{n+1} = \mathcal{K}_n(y_{n+1})$, $y_{n+1}^p - y_{n+1} = z_n + \beta_{n+1}$ con $z_n \in \mathcal{K}_n$ y $v_{\mathfrak{p}}(z_n) \geq 0$ para todo divisor \mathfrak{P} que no divide a P . Por tanto, por el proceso de la demostración de la Proposición 11.8.26 se tiene que β_{n+1} tiene la forma requerida. Notemos que puede ser que $\lambda_{n+1} = 0$ pues la codificación de la ramificación de los primos de \mathcal{K}_n sobre P bien se pudiera presentar en z_n . \square

Observación 11.8.28. Hemos desarrollado el caso particular en que la extensión \mathcal{K}/K es cíclica de grado p^n y $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$. En

este caso particular se tiene que $\lambda_1 > 0$ pues P es totalmente ramificado en \mathcal{K}/K . Sin embargo la Proposición 11.8.26 y el Corolario 11.8.27 pueden ser generalizados de manera natural a una extensión arbitrara \mathcal{K}/K cíclica de grado p^n . En este caso tenemos

(I) Para $n = 1$, $\mathcal{K} = K(y)$ con $y^p - y = h(T) \in K$ y tal que

$$(h(T))_K = \frac{\mathfrak{C}}{\mathfrak{p}_1^{\lambda_1} \cdots \mathfrak{p}_r^{\lambda_r}} \quad \text{con} \quad \text{mcd}(\mathfrak{C}, \mathfrak{p}_i) = 1, \quad 1 \leq i \leq r, \\ \lambda_i > 0 \quad \text{y} \quad \text{mcd}(\lambda_i, p) = 1.$$

Los primos ramificados son precisamente $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

(II) Para n arbitraria, $\mathcal{K} = K(\mathbf{y})$, $\mathbf{y}^p \stackrel{\bullet}{=} \mathbf{y} = \boldsymbol{\beta} \in W_n(K)$ tal que

$$(\beta_i)_K = \frac{\mathfrak{C}_i}{\mathfrak{p}_1^{\lambda_{1,i}} \cdots \mathfrak{p}_r^{\lambda_{r,i}}} \quad \text{con} \quad \lambda_{j,i} \geq 0 \quad \text{y si} \quad \lambda_{j,i} > 0, \\ \text{mcd}(\mathfrak{C}_i, \mathfrak{p}_j) = 1 \quad \text{y} \quad \text{mcd}(\lambda_{j,i}, p) = 1.$$

El índice de ramificación de cada \mathfrak{p}_j es p^{n-i+1} donde i es el primer índice i tal que $\lambda_{j,i} > 0$. En otras palabras, \mathfrak{p}_j es no ramificado en $\mathcal{K}_{i-1} := K(y_1, \dots, y_{i-1})/K$ y totalmente ramificado en $\mathcal{K} = \mathcal{K}_n/\mathcal{K}_i$.

H. L. Schmid introdujo los siguientes invariantes. Sea \mathcal{K}/K una extensión cíclica de grado p^n con $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$. Sea $\mathcal{K} = K(\mathbf{y})$ tal que $\mathbf{y}^p \stackrel{\bullet}{=} \mathbf{y} = \boldsymbol{\beta} \in W_n(K)$, $(\beta_i) = \frac{\mathfrak{C}_i}{\mathfrak{p}^{\lambda_i}}$ con $\lambda_i \geq 0$ y si $\lambda_i > 0$ entonces $\text{mcd}(\mathfrak{C}_i, \mathfrak{p}) = 1$ y $\text{mcd}(\lambda_i, p) = 1$ donde \mathfrak{p} es el divisor asociado a P .

Sea $M_n := \max_{1 \leq i \leq n} \{p^{n-i}\lambda_i\}$. Notemos que $M_i = \max\{pM_{i-1}, \lambda_i\}$, $M_1 < M_2 < \cdots < M_n$ y que el valor máximo se alcanza en un único $p^{n-i}\lambda_i$ pues si $p^{n-i}\lambda_i = p^{n-j}\lambda_j$ con $j > i$, entonces $p^{j-i}\lambda_i = \lambda_j$ pero esto contradice que $\text{mcd}(p, \lambda_j) = 1$.

Teorema 11.8.29. *Con las condiciones anteriores, se tiene que el conductor de \mathcal{K}/K es*

$$\mathfrak{f}_{\mathcal{K}} = P^{M_n+1}.$$

Demostración. [65, p. 163]. □

Corolario 11.8.30. *Sea \mathcal{K}/K una extensión cíclica de grado p^n con $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$. Entonces $M_n + 1 \leq \alpha$.*

Demostración. Se sigue inmediatamente del Lema 11.8.24 y del Teorema 11.8.29. □

El teorema de Kronecker–Weber en característica p y campos de géneros

12.1. Introducción

El teorema clásico de Kronecker–Weber establece que toda extensión finita \mathbb{Q} está contenida en un campo ciclotómico. Equivalentemente, la máxima extensión abeliana de \mathbb{Q} es la unión de todos los campos ciclotómicos. En 1974 D. Hayes [25], probó el resultado análogo para campos de funciones racionales congruentes. Tenemos que la unión de todos los campos de funciones ciclotómicos no es la máxima extensión abeliana del campo de funciones racionales congruente $K = \mathbb{F}_q(T)$ puesto que todas estas extensiones son geométricas y el primo infinito es moderadamente ramificado. Hayes probó que la máxima extensión abeliana de K es la composición de la unión de todos los campos de funciones ciclotómicos con la unión de todas las extensiones de constantes y con la unión de los subcampos del campo de funciones ciclotómico para el primo infinito donde el primo infinito es total y salvajemente ramificado. La demostración de Hayes usa teoría de campos de clase.

La demostración del caso clásico la dimos en el Capítulo 4 la cual usa grupos de ramificación. La herramienta clave en la demostración es que hay una única extensión cíclica de \mathbb{Q} de grado p (p impar), y p es el único primo ramificado. En el caso de campos de funciones racionales la situación es bastante diferente. Existen muchas extensiones cíclicas de K de grado p donde únicamente un divisor primo es ramificado.

En la primera parte de este capítulo se presenta una demostración del análogo al Teorema de Kronecker–Weber para campos de funciones racionales congruentes usando argumentos de conteo en el caso de ramificación salvaje. Primero, como en el caso clásico, mostramos que cualquier extensión cíclica de K está contenida en la composición de un campo de funciones ciclotómicos y una extensión de constantes. El siguiente paso, el fundamental, es mostrar que toda extensión cíclica de grado una potencia de p donde únicamente hay un primo ramificado y éste es completamente ramificado, está contenida en un campo de funciones ciclotómica. Una vez que esto esté probado, el resto

de la prueba se sigue fácilmente. Usamos la aritmética de vectores de Witt desarrollada por Schmid en [65] (ver Capítulo 11).

En la segunda parte de este capítulo desarrollamos un análogo a la teoría de Leopoldt del género para campos de funciones congruentes. Se da una descripción del campo de géneros $\mathcal{K}\mathbf{gc}$ de una extensión abeliana finita de un campo de funciones racionales congruente por medio de su grupo de caracteres de Dirichlet en campos de funciones ciclotómicos. Aquí consideramos el campo de clases de Hilbert \mathcal{K}_H de un campo de funciones \mathcal{K} usando la construcción de Rosen para $S_\infty = \{\mathfrak{p}_\infty\}$, donde \mathfrak{p}_∞ es el divisor de polos de T en el campo de funciones racionales $K = \mathbb{F}_q(T)$.

Más precisamente, sea \mathcal{K} una extensión abeliana finita de K . Entonces, si \mathcal{K} está contenido en una extensión ciclotómica, se encuentra que $\mathcal{K}\mathbf{gc}$ también está contenido en una extensión ciclotómica y se encuentra el grupo de caracteres de Dirichlet asociado a $\mathcal{K}\mathbf{gc}$. Si \mathcal{K} no está contenido en una extensión ciclotómica y \mathfrak{p}_∞ es moderadamente ramificado, se considera una extensión adecuada de constantes de \mathcal{K} y entonces se procede como antes para hallar $\mathcal{K}\mathbf{gc}$. Finalmente, si \mathfrak{p}_∞ es salvajemente ramificado, se considera la extensión ciclotómica donde \mathfrak{p}_∞ es total y salvajemente ramificado y se procede de manera similar a los casos previos.

Aplicamos los resultados obtenidos a extensiones de Kummer y de Artin–Schreier de K . Al final se muestra que la construcción dada también funciona para hallar explícitamente el campo de géneros de una extensión p -cíclica arbitraria de K dada por un vector de Witt.

12.2. El Teorema de Kronecker–Weber para campos de funciones

Para esta sección establecemos nuevamente la notación que usaremos. Sea $K_T := \bigcup_{M \in R_T} K(\Lambda_M)$, $\mathbb{F}_\infty := \bigcup_{m \in \mathbb{N}} \mathbb{F}_{q^m}$. Denotamos por \mathfrak{p}_∞ el divisor de polos de T en \bar{K} . Denotamos por L_n al máximo subcampo de $K(\Lambda_{1/T^n})$ donde \mathfrak{p}_∞ es total y salvajemente ramificado, $n \in \mathbb{N}$. Sea $L_\infty := \bigcup_{n \in \mathbb{N}} L_n$.

El principal objetivo de este capítulo es probar el siguiente resultado.

Teorema 12.2.1 (Kronecker–Weber, [25], [70, Theorem 12.8.31]). *La máxima extensión abeliana A de K es $A = K_T \mathbb{F}_\infty L_\infty$.* \square

Para probar el Teorema 12.2.1 es suficiente probar que toda extensión abeliana finita de K está contenida en $K(\Lambda_N) \mathbb{F}_{q^m} L_n$ para algunos $N \in R_T$, y $m, n \in \mathbb{N}$.

Sea L/K una extensión abeliana finita. Sea $G := \text{Gal}(L/K) \cong C_{n_1} \times \cdots \times C_{n_l} \times C_{p^{a_1}} \times \cdots \times C_{p^{a_h}}$ donde $\text{mcd}(n_i, p) = 1$, $1 \leq i \leq l$ y $a_j \in \mathbb{N}$, $1 \leq j \leq h$. Sea $S_i \subseteq L$ tal que $\text{Gal}(S_i/K) \cong C_{n_i}$, $1 \leq i \leq l$ y sea $R_j \subseteq L$ tal que $\text{Gal}(R_j/K) \cong C_{p^{a_j}}$, $1 \leq j \leq h$. Para probar el Teorema 12.2.1 es

suficiente mostrar que cada S_i y cada R_j están contenidos en $K(A_N)\mathbb{F}_{q^m}L_n$ para algunas $N \in R_T, m, n \in \mathbb{N}$.

En resumen, podemos suponer que L/K es una extensión cíclica de grado h donde ya sea $\text{mcd}(h, p) = 1$ o $h = p^n$ para algún $n \in \mathbb{N}$.

12.2.1. Extensiones geométricas moderadamente ramificadas

En esta subsección probaremos el Teorema 12.2.1 para el caso particular de una extensión moderadamente ramificada. Sea L/K una extensión abeliana. Sea $P \in R_T$, $d := \text{gr } P$.

Proposición 12.2.2. *Sea P moderadamente ramificado en L/K . Si e denota el índice de ramificación de P en L , tenemos $e \mid q^d - 1$.*

Demostración. Primero consideramos en general una extensión abeliana L/K . Sean $G_{-1} = D$ el grupo de descomposición de P , $G_0 = I$ el grupo de inercia y $G_i, i \geq 1$, los grupos de ramificación. Sea \mathfrak{P} un divisor primo en L que divide a P . Entonces si $\mathcal{O}_{\mathfrak{P}}$ denota el anillo de valuación de \mathfrak{P} , tenemos

$$U^{(i)} = 1 + \mathfrak{P}^i \subseteq \mathcal{O}_{\mathfrak{P}}^* = \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P}, i \geq 1, U^{(0)} = \mathcal{O}_{\mathfrak{P}}^*.$$

Sea $l(\mathfrak{P}) := \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ el campo residual en \mathfrak{P} . Los siguientes mapeos φ_i son monomorfismos de grupos:

$$G_i/G_{i+1} \xrightarrow{\varphi_i} U^{(i)}/U^{(i+1)} \cong \begin{cases} l(\mathfrak{P})^*, i = 0 \\ \mathfrak{P}^i/\mathfrak{P}^{i+1} \cong l(\mathfrak{P}), i \geq 1. \end{cases}$$

$$\bar{\sigma} \mapsto \sigma\pi/\pi$$

donde π denota un elemento primo para \mathfrak{P} .

Probaremos el análogo a la Proposición 1.3.12 para campos de funciones, esto es, si $G_{-1}/G_1 = D/G_1$ es abeliano, entonces

$$\varphi = \varphi_0: G_0/G_1 \longrightarrow U^{(0)}/U^{(1)} \cong (\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})^*$$

satisface que $\text{im } \varphi \subseteq \mathcal{O}_P/(P) \cong R_T/(P) \cong \mathbb{F}_{q^d}$. En particular se seguirá que $|G_0/G_1| \mid |\mathbb{F}_{q^d}^*| = q^d - 1$.

Para demostrar esta afirmación, notemos que

$$\text{Aut}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_P/(P))) \cong \text{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_P/(P))) = D/I = G_{-1}/G_0$$

(ver [70, Corollary 5.2.12]).

Sea $\sigma \in G_0$ y $\varphi(\bar{\sigma}) = \varphi(\sigma \text{ mód } G_1) = [\alpha] \in (\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})^*$. Esto es, $\varphi(\bar{\sigma}) = \sigma\pi/\pi \text{ mód } \mathfrak{P} = [\alpha]$. Por lo tanto $\sigma\pi \equiv \alpha\pi \text{ mód } \mathfrak{P}^2$.

Sea $\theta \in G_{-1} = D$ arbitraria y sea $\pi_1 := \theta^{-1}\pi$. Entonces π_1 es un elemento primo para \mathfrak{P} . Puesto que φ es independiente del elemento primo, se sigue que $\sigma\pi_1 \equiv \alpha\pi_1 \text{ mód } \mathfrak{P}^2$, es decir, $\sigma\theta^{-1}\pi \equiv \alpha\theta^{-1}\pi \text{ mód } \mathfrak{P}^2$. Puesto G_{-1}/G_1 es un grupo abeliano, tenemos

$$\sigma\pi = (\theta\sigma\theta^{-1})(\pi) \equiv \theta(\alpha)\pi \text{ mód } \mathfrak{P}^2.$$

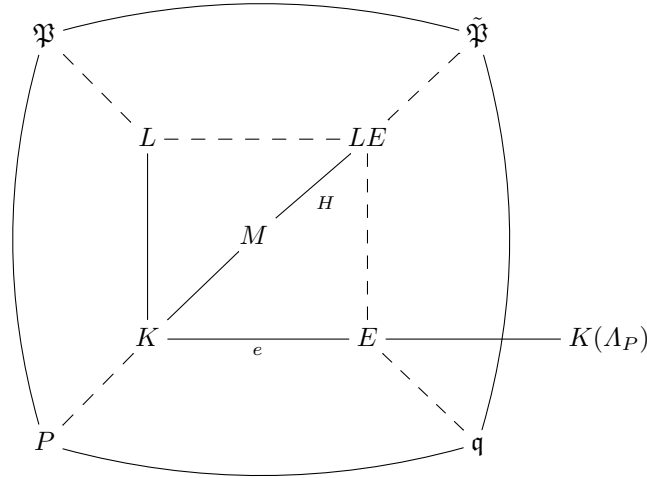
Por lo tanto $\sigma\pi \equiv \theta(\alpha)\pi \text{ mód } \mathfrak{P}^2$ y $\sigma\pi \equiv \alpha\pi \text{ mód } \mathfrak{P}^2$. Se sigue que $\theta(\alpha) \equiv \alpha \text{ mód } \mathfrak{P}$ para toda $\theta \in G_{-1}$.

Si escribimos $\tilde{\theta} := \theta \text{ mód } G_0$, se tiene que $\tilde{\theta}[\alpha] = [\alpha]$, esto es, $[\alpha]$ es un elemento fijo bajo la acción del grupo $G_{-1}/G_0 \cong \text{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_P/(P)))$. Se obtiene que $[\alpha] \in \mathcal{O}_P/(P)$. Luego $\text{im } \varphi \subseteq (\mathcal{O}_P/(P))^*$ y $|G_0/G_1| \mid |(\mathcal{O}_P/(P))^*| = q^d - 1$.

Finalmente, puesto que L/K es abeliana y P es moderadamente ramificada, tenemos que $G_1 = \{1\}$ y por tanto se sigue que $e = |G_0| = |G_0/G_1| \mid q^d - 1$. \square

Ahora consideremos una extensión abeliana finita moderadamente ramificada L/K donde P_1, \dots, P_r donde son los primos finitos ramificados. Sean $P \in \{P_1, \dots, P_r\}$ y e el índice de ramificación de P en L . Entonces, como consecuencia de la Proposición 12.2.2, tenemos que $e \mid q^d - 1$. Ahora bien, P es totalmente ramificado en $K(\Lambda_P)/K$ con índice de ramificación $q^d - 1$. En esta extensión \mathfrak{p}_∞ tiene índice de ramificación igual a $q - 1$.

Sea $K \subseteq E \subseteq K(\Lambda_P)$ con $[E : K] = e$. Pongamos $\tilde{\mathfrak{P}}$ un divisor primo en LE que divide a P . Sean $\mathfrak{q} := \tilde{\mathfrak{P}}|_E$ y $\mathfrak{P} := \tilde{\mathfrak{P}}|_L$.



Tenemos que $e = e_{L/K}(\mathfrak{P}|P) = e_{E/K}(\mathfrak{q}|P)$. Como consecuencia del Lema de Abhyankar [70, Theorem 12.4.4], se obtiene que

$$e_{LE/K}(\tilde{\mathfrak{P}}|P) = \text{mcm}[e_{L/K}(\mathfrak{P}|P), e_{E/K}(\mathfrak{q}|P)] = \text{mcm}[e, e] = e.$$

Sea $H \subseteq \text{Gal}(LE/K)$ el grupo de inercia de $\tilde{\mathfrak{P}}/P$. Pongamos $M := (LE)^H$. Entonces P es no ramificado en la extensión M/K . Queremos probar que $L \subseteq MK(\Lambda_P)$. De hecho se tiene que $[LE : M] = e$ y $E \cap M = K$ puesto que P es totalmente ramificado en E/K y no ramificado en M/K . Se sigue que $[ME : K] = [M : K][E : K]$. Luego

$$[LE : K] = [LE : M][M : K] = e \frac{[ME : K]}{[E : K]} = e \frac{[ME : K]}{e} = [ME : K].$$

Puesto que $ME \subseteq LE$ se sigue que $LE = ME \subseteq MK(\Lambda_P)$. Por tanto $L \subseteq MK(\Lambda_P)$.

En M/K los primos finitos ramificados son $\{P_2, \dots, P_r\}$. En caso de que $r - 1 \geq 1$ podemos aplicar el argumento anterior a M/K obteniendo de esta forma una extensión M_2/K de tal manera que a lo más $r - 2$ primos finitos de K son ramificados en M_2K y se tiene que $M \subseteq M_2K(\Lambda_{P_2})$, por lo que $L \subseteq MK(\Lambda_{P_1}) \subseteq M_2K(\Lambda_{P_1})K(\Lambda_{P_2})$.

Llevando a cabo el proceso anterior a lo más r veces, obtenemos

$$L \subseteq M_0K(\Lambda_{P_1 P_2 \dots P_r}) \quad (12.1)$$

en donde en la extensión M_0/K el único posible primo ramificado es \mathfrak{p}_∞ .

El siguiente resultado nos describe el campo M_0 .

Proposición 12.2.3. *Sea L/K una extensión abeliana donde a lo más un divisor primo \mathfrak{p} de grado 1 es ramificado y la extensión es moderadamente ramificada. Entonces L/K es una extensión de constantes.*

Demostración. Por la Proposición 12.2.2 tenemos que $e := e_{L/K}(\mathfrak{p})|q - 1$. Sea H el grupo de inercia de \mathfrak{p} . Entonces $|H| = e$ y \mathfrak{p} es no ramificado en $E := L^H/K$. Por tanto E/K es una extensión no ramificada de donde se sigue que E/K es una extensión de constantes.

Sea $[E : K] = m$, $E = K\mathbb{F}_{q^m}$. Entonces si \mathfrak{P} es un divisor primo en E que divide a \mathfrak{p} se tiene que el grado relativo $d_{E/K}(\mathfrak{P}|\mathfrak{p})$ es igual a m , el número de divisores primos en E/K sobre \mathfrak{p} es uno y el grado de \mathfrak{P} es uno (ver [70, Theorem 6.2.1]). Por lo tanto \mathfrak{P} es el único divisor primo ramificado en L/E y es de grado uno y totalmente ramificado. Más aún $[L : E] = e \mid q^m - 1 = |\mathbb{F}_{q^m}^*|$.

Las $(q^m - 1)$ -ésimas raíces de la unidad pertenecen a $\mathbb{F}_{q^m} \subseteq E$. De aquí se tiene que E contiene las e -ésimas raíces de la unidad y L/E es una extensión de Kummer, digamos $L = E(y)$ con $y^e = \alpha \in E = \mathbb{F}_{q^m}K = \mathbb{F}_{q^m}(T)$. Escribimos α en la forma normal prescrita por Hasse ([20] y Observación 11.8.28): $(\alpha)_E = \frac{\mathfrak{p}^a}{\mathfrak{b}}$, $0 < a < e$. Ahora bien, puesto $\text{gr}(\alpha)_E = 0$ se sigue que $\text{gr}_E \mathfrak{a}$ o $\text{gr}_E \mathfrak{b}$ no es un múltiplo de e . Esto contradice que \mathfrak{p} es el único primo ramificado. Por lo tanto $L = E$ y L/K es una extensión de constantes. \square

Como corolario a (12.1) y a la Proposición 12.2.3 obtenemos el Teorema 12.2.1 para el caso moderadamente ramificado.

Corollary 12.2.4. *Si L/K es una extensión finita abeliana moderadamente ramificada donde los divisores primos finitos ramificados son P_1, \dots, P_r , entonces*

$$L \subseteq \mathbb{F}_{q^m}K(\Lambda_{P_1 \dots P_r}).$$

para alguna $m \in \mathbb{N}$. \square

12.2.2. Extensiones salvajemente ramificadas

Reducciones

Como consecuencia del Corolario 12.2.4, el Teorema 12.2.1 se seguirá si probamos el caso particular de una extensión cíclica \mathcal{K}/K de grado p^n para alguna $n \in \mathbb{N}$. Ahora, este tipo de extensiones están dadas por medio de un vector de Witt:

$$\mathcal{K} = K(\mathbf{y}) = K(y_1, \dots, y_n) \quad \text{con} \quad \mathbf{y}^p \cdot \mathbf{y} = \boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in W_n(K).$$

Primero consideremos una extensión de Artin–Schreier. Sea $\mathcal{K} := K(y)$ donde $y^p - y = \alpha \in K$. La ecuación puede ser normalizada como sigue:

$$y^p - y = \alpha = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}} + f(T), \quad (12.2)$$

donde $P_i \in R_T^+$, $Q_i \in R_T$, $\text{mcd}(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\text{gr } Q_i < \text{gr } P_i^{e_i}$, $1 \leq i \leq r$, $f(T) \in R_T$, con $p \nmid \text{gr } f$ cuando $f(T) \notin \mathbb{F}_q$.

Tenemos que los primos finitos ramificados en \mathcal{K}/K son precisamente P_1, \dots, P_r . Con respecto a \mathfrak{p}_∞ tenemos

Proposición 12.2.5. *El primo \mathfrak{p}_∞ es*

- (I) *descompuesto si $f(T) = 0$.*
- (II) *inerte si $f(T) \in \mathbb{F}_q$ y $f(T) \notin \wp(\mathbb{F}_q) := \{a^p - a \mid a \in \mathbb{F}_q\}$.*
- (III) *ramificado si $f(T) \notin \mathbb{F}_q$ (por tanto $p \nmid \text{gr } f$).*

Demostración. Primero consideremos el caso $f(T) = 0$. Entonces $v_{\mathfrak{p}_\infty}(\alpha) = \text{gr}(P_1^{e_1} \cdots P_r^{e_r}) - \text{gr } Q > 0$. Por lo tanto \mathfrak{p}_∞ es no ramificado. Ahora $y^p - y = \prod_{i=0}^{p-1} (y - i)$. Sea $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$. Entonces

$$v_{\mathfrak{P}_\infty}(y^p - y) = \sum_{i=0}^{p-1} v_{\mathfrak{P}_\infty}(y - i) = e(\mathfrak{P}_\infty \mid \mathfrak{p}_\infty) v_{\mathfrak{p}_\infty}(\alpha) = v_{\mathfrak{p}_\infty}(\alpha) > 0.$$

Se sigue que existe $0 \leq i \leq p-1$ tal que $v_{\mathfrak{P}_\infty}(y - i) > 0$. Sin pérdida de generalidad podemos suponer $i = 0$. Sea $\sigma \in \text{Gal}(\mathcal{K}/K) \setminus \{\text{Id}\}$. Supongamos que $\mathfrak{P}_\infty^\sigma = \mathfrak{P}_\infty$. Let $y^\sigma = y - j$, $j \neq 0$. Entonces, por un lado tenemos

$$v_{\mathfrak{P}_\infty}(y - j) = v_{\mathfrak{P}_\infty}(y^\sigma) = v_{\sigma(\mathfrak{P}_\infty)}(y) = v_{\mathfrak{P}_\infty}(y) > 0.$$

Por otro lado, puesto que $v_{\mathfrak{P}_\infty}(y) > 0 = v_{\mathfrak{P}_\infty}(j)$, se sigue que

$$v_{\mathfrak{P}_\infty}(y - j) = \min\{v_{\mathfrak{P}_\infty}(y), v_{\mathfrak{P}_\infty}(j)\} = 0.$$

Por lo tanto $\mathfrak{P}_\infty^\sigma \neq \mathfrak{P}_\infty$ y entonces \mathfrak{p}_∞ se descompone en \mathcal{K}/K .

Ahora consideremos el caso $f(T) \neq 0$. Si $f(T) \notin \mathbb{F}_q$, entonces $f(T)$ se ramifica pues está en la forma normal preescrita por Hasse [20] (ver la demostración de la Proposición 11.8.26).

El último caso es cuando $f(T) \in \mathbb{F}_q$, $f(T) \notin \wp(\mathbb{F}_q)$. Sea $b \in \mathbb{F}_{q^p}$ con $b^p - b = a = f(T)$. Puesto que $\text{gr } \mathfrak{p}_\infty = 1$, \mathfrak{p}_∞ es inerte en extensiones de constantes $K(b)/K$ ([70, Theorem 6.2.1]). Supongamos que \mathfrak{p}_∞ se descompone en $K(y)/K$. Tenemos el siguiente diagrama

$$\begin{array}{ccc} K(y) & \xrightarrow[\text{inerte}]{\mathfrak{p}_\infty} & K(y, b) \\ \mathfrak{p}_\infty \text{ descompuesto} \downarrow & & \downarrow \\ K & \xrightarrow[\text{inerte}]{\mathfrak{p}_\infty} & K(b) \end{array}$$

Se sigue que el grupo de descomposición de \mathfrak{p}_∞ en $K(y, b)/K$ es $D = \text{Gal}(K(y, b)/K(y))$. Por lo tanto \mathfrak{p}_∞ es inerte en cualquier otro campo de grado p sobre K diferente a $K(y)$. Tenemos que los campos de grado p son $K(y + ib), K(b)$, $0 \leq i \leq p-1$. En $K(y + b)/K$ tenemos

$$(y + b)^p - (y + b) = (y^p - y) + (b^p - b) = \alpha - a = \frac{Q}{P_1^{e_1} \dots P_r^{e_r}}$$

con $\text{gr}(\alpha - a) < 0$. Por tanto, por la primera parte, \mathfrak{p}_∞ se descompone en $K(y + b)/K$ y en $K(y)/K$ lo cual es imposible. Por tanto \mathfrak{p}_∞ es inerte en $K(y)/K$. \square

El siguiente teorema nos prueba que en una extensión cíclica de grado p^n dada por un vector de Witt, podemos separar cada primo ramificado. Más precisamente, tenemos:

Teorema 12.2.6. *Sea \mathcal{K}/K una extensión cíclica de grado p^n donde se tiene que $P_1, \dots, P_r \in R_T^+$ y posiblemente \mathfrak{p}_∞ , son los divisores primos ramificados. Entonces $\mathcal{K} = K(\mathbf{y})$ donde*

$$\mathbf{y}^p \dot{-} \mathbf{y} = \boldsymbol{\beta} = \boldsymbol{\delta}_1 \dot{+} \dots \dot{+} \boldsymbol{\delta}_r \dot{+} \boldsymbol{\mu},$$

con $\beta_1^p - \beta_1 \notin \wp(K)$, $\delta_{ij} = \frac{Q_{ij}}{P_i^{e_{ij}}}$, $e_{ij} \geq 0$, $Q_{ij} \in R_T$ y

(I) si $e_{ij} = 0$ entonces $Q_{ij} = 0$;

(II) si $e_{ij} > 0$ entonces $p \nmid e_{ij}$, $\text{mcd}(Q_{ij}, P_i) = 1$ y $\text{gr}(Q_{ij}) < \text{gr}(P_i^{e_{ij}})$,

y $\mu_j = f_j(T) \in R_T$ con

(III) $p \nmid \text{gr } f_j$ cuando $f_j \notin \mathbb{F}_q$ y

(IV) $\mu_j \notin \wp(\mathbb{F}_q) := \{a^p - a \mid a \in \mathbb{F}_q\}$ cuando $\mu_j \in \mathbb{F}_q^*$.

Demostración. Consideremos \mathcal{K}/K una extensión cíclica de grado p^n definida por $\mathcal{K} := K(\mathbf{y})$, $\mathbf{y}^p \dot{-} \mathbf{y} = \boldsymbol{\beta}$ con $\mathbf{y} \in W_n(\mathcal{K})$ un vector de Witt de longitud n en \mathcal{K} y $\boldsymbol{\beta} \in W_n(K)$ un vector de Witt de longitud n en K .

Sea $\beta = (\beta_1, \dots, \beta_n)$ tal que

$$\beta_j = \sum_{i=1}^r \frac{Q_{ij}}{P_i^{e_{ij}}} + f_j(T), \text{ donde } P_1, \dots, P_r \in R_T^+, \{Q_{ij}\}_{1 \leq i \leq r}^{1 \leq j \leq n} \subseteq R_T, \\ f_j(T) \in R_T, e_{ij} \in \mathbb{N} \cup \{0\} \text{ para toda } 1 \leq i \leq r \text{ y } 1 \leq j \leq n. \quad (12.3)$$

Sea φ definido como en (11.2). Aplicando φ a β obtenemos $(\beta^{(1)}, \dots, \beta^{(n)})$ y de la definición de $\beta^{(j)}$, se tiene que que estos elementos son de la forma

$$\beta^{(j)} = \sum_{i=1}^r \frac{Q'_{ij}}{P_i^{e'_{ij}}} + f'_j(T) \text{ para todo } 1 \leq j \leq n.$$

Escribamos

$$\beta = \gamma_1 + \dots + \gamma_r + \xi, \\ (\beta^{(1)}, \dots, \beta^{(n)}) = (\gamma_1^{(1)}, \dots, \gamma_1^{(n)}) + \dots + (\gamma_r^{(1)}, \dots, \gamma_r^{(n)}) + (\xi^{(1)}, \dots, \xi^{(n)})$$

con

$$\gamma_i^{(j)} = \frac{Q'_{ij}}{P_i^{e'_{ij}}}, \quad 1 \leq i \leq r, \quad 1 \leq j \leq n \quad \text{y} \quad \xi^{(j)} = f'_j(T).$$

Cuando aplicamos φ^{-1} , obtenemos

$$(\beta_1, \dots, \beta_n) = (\beta^{(1)}, \dots, \beta^{(n)})^{\varphi^{-1}} = (\gamma_1)^{\varphi^{-1}} \dot{+} \dots \dot{+} (\gamma_r)^{\varphi^{-1}} \dot{+} (\xi)^{\varphi^{-1}}$$

y cada vector $(\gamma_i)^{\varphi^{-1}}$ es de la forma $\left(\frac{Q'_{i1}}{P_i^{e'_{i1}}}, \dots, \frac{Q'_{in}}{P_i^{e'_{in}}}\right)$ y el vector $(\xi)^{\varphi^{-1}}$ es de la forma $(f''_1(T), \dots, f''_n(T))$. En otras palabras

$$\beta = \delta_1 \dot{+} \dots \dot{+} \delta_r \dot{+} \mu$$

en donde las componentes de cada δ_i tienen polos a lo más en P_i y μ tiene componentes con polos a lo más en \mathfrak{p}_∞ . Sea \mathfrak{p}_i el divisor correspondiente a P_i .

Ahora cada δ y μ pueden ser normalizados de manera que cada componente $(\delta_i)_j := \delta_{ij}$ tiene divisor

$$(\delta_{ij})_K = \frac{\mathfrak{a}_{ij}}{\mathfrak{p}_i^{\lambda_i}} \text{ con } \lambda_i \geq 0; \text{ si } \lambda_i = 0, \text{ entonces } v_{\mathfrak{p}_i}(\mathfrak{a}_{ij}) \geq 0; \\ \text{si } \lambda_i > 0, \text{ entonces } \text{mcd}(p, \lambda_i) = 1 \text{ y } v_{\mathfrak{p}_{ij}}(\mathfrak{a}_{ij}) = 0 \quad (12.4)$$

y similarmente para μ con respecto a \mathfrak{p}_∞ (ver [65, página 62] y Observación 11.8.28). De hecho, la normalización puede ser obtenida mediante el cambio de variable $\mathbf{y}_i \mapsto \mathbf{y}_i \dot{+} \boldsymbol{\alpha}_i$ la cual corresponde a la substitución $\delta_i \mapsto \delta_i \dot{+}$

$\alpha_i^p \dot{-} \alpha_i$ y por lo tanto las componentes de cada α_i no tiene otro polo que no sea \mathfrak{p}_i . Más directamente, en el nivel j , aplicando la técnica de Hasse, una sustitución $y_j \rightarrow y_j + \xi_j$ nos lleva a la normalización de δ_{ij} en la forma normal dada en (12.4). \square

Ahora estudiamos el comportamiento de \mathfrak{p}_∞ en \mathcal{K}/K .

Proposición 12.2.7. *Sea \mathcal{K}/K dado como el en Teorema 12.2.6. Sea $\mu_1 = \dots = \mu_s = 0$, $\mu_{s+1} \in \mathbb{F}_q^*$, $\mu_{s+1} \notin \wp(\mathbb{F}_q)$ y finalmente sea $t+1$ el primer índice con $f_{t+1} \notin \mathbb{F}_q$ (y por lo tanto $p \nmid \text{gr } f_{t+1}$). Entonces el índice de ramificación de \mathfrak{p}_∞ es p^{n-t} , el grado de inercia de \mathfrak{p}_∞ es p^{t-s} y el número de descomposición de \mathfrak{p}_∞ es p^s . Más precisamente, si $\text{Gal}(\mathcal{K}/K) = \langle \sigma \rangle \cong C_{p^n}$, entonces el grupo de inercia de \mathfrak{p}_∞ es $\mathfrak{I} = \langle \sigma^{p^t} \rangle$ y el grupo de descomposición de \mathfrak{p}_∞ es $\mathfrak{D} = \langle \sigma^{p^s} \rangle$.*

Demostración. Puesto que la extensión \mathcal{K}/K es una extensión de Galois de orden una potencia de un número primo, el campo de inercia es el primer nivel en donde \mathfrak{p}_∞ se ramifica. El índice de este primer nivel es $t+1$ (ver [65] y Observación 11.8.28). Por otro lado, por la misma razón, el campo de descomposición es el primer nivel donde \mathfrak{p}_∞ es inerte y este está dado por $s+1$ (Proposición 12.2.5). \square

Consideremos el campo $\mathcal{K} = K(\mathbf{y})$ como en el Teorema 12.2.6, donde únicamente un divisor prime $P \in R_T^+$ se ramifica, con

$$\begin{aligned} \beta_i &= \frac{Q_i}{P^{\lambda_i}}, Q_i \in R_T \text{ tal que } \lambda_i \geq 0, \\ \text{si } \lambda_i &= 0 \text{ entonces } Q_i = 0, \\ \text{si } \lambda_i &> 0 \text{ entonces } \text{mcm}(\lambda_i, p) = 1, \text{mcd}(Q_i, P) = 1 \text{ y } \text{gr } Q_i < \text{gr } P^{\lambda_i}, \\ \lambda_1 &> 0. \end{aligned} \tag{12.5}$$

Un caso particular del Teorema 12.2.6 adecuado para nuestro estudio se da en la siguiente proposición.

Proposición 12.2.8. *Supongamos que toda extensión \mathcal{K}_1/K que cumpla con las condiciones de (12.5) satisface que $\mathcal{K}_1 \subseteq K(\Lambda_{P^\alpha})$ para alguna $\alpha \in \mathbb{N}$. Sea \mathcal{K}/K la extensión definida por $\mathcal{K} = K(\mathbf{y})$ donde $\wp(\mathbf{y}) = \mathbf{y}^p \dot{-} \mathbf{y} = \boldsymbol{\beta}$ con $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$, β_i dado en forma normal: $\beta_i \in \mathbb{F}_q$ o $\beta_i = \frac{Q_i}{P^{\lambda_i}}$, $Q_i \in R_T$ y $\lambda_i > 0$, $\text{mcd}(\lambda_i, p) = 1$, $\text{mcd}(Q_i, P) = 1$ y $\text{gr } Q_i \leq \text{gr } P^{\lambda_i}$. Entonces $\mathcal{K} \subseteq \mathbb{F}_{q^{p^n}} K(\Lambda_{P^\alpha})$ para alguna $\alpha \in \mathbb{F}_q$.*

Demostración. Del Teorema 12.2.6 se tiene que podemos descomponer el vector $\boldsymbol{\beta}$ como $\boldsymbol{\beta} = \boldsymbol{\varepsilon} \dot{+} \boldsymbol{\gamma}$ con $\varepsilon_i \in \mathbb{F}_q$ para toda $1 \leq i \leq n$ y $\gamma_i = 0$ o $\gamma_i = \frac{Q_i}{P^{\lambda_i}}$, $Q_i \in R_T$ y $\lambda_i > 0$, $\text{mcd}(\lambda_i, p) = 1$, $\text{mcd}(Q_i, P) = 1$ y $\text{gr } Q_i < \text{gr } P^{\lambda_i}$.

Sea $\gamma_1 = \dots = \gamma_r = 0$, y $\gamma_{r+1} \notin \mathbb{F}_q$. Tenemos $\mathcal{K} \subseteq K(\boldsymbol{\varepsilon})K(\boldsymbol{\gamma})$. Ahora $K(\boldsymbol{\varepsilon}) \subseteq \mathbb{F}_{q^{p^n}}$ y $K(\boldsymbol{\gamma}) = K(0, \dots, 0, \gamma_{r+1}, \dots, \gamma_n)$.

Para cualquier vector de Witt $\mathbf{x} = (x_1, \dots, x_n)$ tenemos la descomposición dada por la Proposición 11.4.3

$$\mathbf{x} = (x_1, 0, 0, \dots, 0) \dot{+} (0, x_2, 0, \dots, 0) \dot{+} \dots \dot{+} (0, \dots, 0, x_j, 0, \dots, 0) \dot{+} (0, \dots, 0, x_{j+1}, \dots, x_n)$$

para cada $0 \leq j \leq n-1$. Se sigue que $K(\gamma) = K(\gamma_{r+1}, \dots, \gamma_n)$. Puesto que este campo satisface las condiciones de (12.5), tenemos $K(\gamma) \subseteq K(\Lambda_{P^\alpha})$ para alguna $\alpha \in \mathbb{N}$. El resultado se sigue. \square

Observación 12.2.9. El primo \mathfrak{p}_∞ puede ser manejado de la misma manera que cualquier $P \in R_T^+$. Las condiciones (12.5) para \mathfrak{p}_∞ son las siguientes. Sea $\mathcal{K} = K(\mu)$ con $\mu_j = f_j(T) \in R_T$, además $f_j(0) = 0$ para toda j y ya sea $f_j(T) = 0$ o $f_j(T) \neq 0$ y $p \nmid \text{gr } f_j(T)$. La condición $f_j(0) = 0$ significa que el primo infinito para $T' = 1/T$ es o descompuesto o ramificado en cada nivel, esto es, el grado de inercia es 1 en \mathcal{K}/K . En este caso, con el cambio de variable $T' = 1/T$ la hipótesis en la Proposición 12.2.8 debe decir que cualquier campo que cumpla estas condiciones satisface que $\mathcal{K} \subseteq K(\Lambda_{T'^m}) = K(\Lambda_{T^{-m}})$ para alguna $m \in \mathbb{N}$. Sin embargo, puesto que el grado de la extensión \mathcal{K}/K es una potencia de p necesariamente tenemos que \mathcal{K} está contenida en $K(\Lambda_{T^{-m}})^{\mathbb{F}_q^*} = L_{m-1}$.

Con las notaciones del Teorema 12.2.6 obtenemos que si $\mathbf{z}_i^p \dot{-} \mathbf{z}_i = \delta_i$, $1 \leq i \leq r$ y si $\mathbf{v}^p \dot{-} \mathbf{v} = \mu$, entonces $\mathcal{K} = K(\mathbf{y}) \subseteq K(\mathbf{z}_1, \dots, \mathbf{z}_r, \mathbf{v}) = K(\mathbf{z}_1) \dots K(\mathbf{z}_r)K(\mathbf{v})$. Por lo tanto, si el Teorema 12.2.1 se cumple para cada $K(\mathbf{z}_i)$, $1 \leq i \leq r$ y para $K(\mathbf{v})$, entonces se cumple para \mathcal{K} .

Del Teorema 12.2.6, de la Proposición 12.2.8 y de la observación después de esta proposición, obtenemos que para probar el Teorema 12.2.1, es suficiente mostrar que cualquier extensión \mathcal{K}/K que cumpla las condiciones de (12.5) satisface que ya sea $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ para alguna $\alpha \in \mathbb{N}$ o $\mathcal{K} \subseteq L_m$ para alguna $m \in \mathbb{N}$. Es suficiente estudiar el caso $P \in R_T^+$.

De las Proposiciones 12.2.5 y 12.2.7 obtenemos

Proposición 12.2.10. Si \mathcal{K} es un campo definido por una ecuación del tipo dado en (12.5), entonces \mathcal{K}/K es una extensión cíclica de grado p^n , P es el único primo ramificado, es totalmente ramificado y \mathfrak{p}_∞ es totalmente descompuesto.

Similarmente, si $\mathcal{K} = K(\mathbf{v})$ donde $v_i = f_i(T) \in R_T$, $f_i(0) = 0$ para toda $1 \leq i \leq n$ y $f_1(T) \notin \mathbb{F}_q$, $p \nmid \text{gr } f_1(T)$, entonces \mathfrak{p}_∞ es el único primo ramificado en \mathcal{K}/K , es totalmente ramificado y el divisor de ceros de T , el cual es ahora el primo al infinito en $R_{1/T}$, es totalmente descompuesto. \square

Hemos reducido la demostración del Teorema 12.2.1 a probar que cualquier extensión del tipo dado en la Proposición 12.2.10 está contenido ya sea en

$K(\Lambda_{P^\alpha})$ para alguna $\alpha \in \mathbb{N}$ o en L_m para alguna $m \in \mathbb{N}$. El segundo caso es consecuencia del primero con el cambio de variable $T' = 1/T$.

Sea $n, \alpha \in \mathbb{N}$. Denotemos por $v_n(\alpha)$ al número de grupos cíclicos de orden p^n contenidos en $(R_T/(P^\alpha))^* \cong \text{Gal}(K(\Lambda_{P^\alpha})/K)$. Tenemos que $v_n(\alpha)$ es el número de extensiones cíclicas \mathcal{K}/K de grado p^n y $\mathcal{K} \subseteq K(\Lambda_{P^\alpha})$. Toda extensión de este tipo satisface que su conductor $\mathfrak{F}_{\mathcal{K}}$ divide a P^α .

Sea ahora $t_n(\alpha)$ el número de extensiones de campos \mathcal{K}/K de grado p^n tal que P es el único primo ramificado, es totalmente ramificado, \mathfrak{p}_∞ es totalmente descompuesto y su conductor $\mathfrak{F}_{\mathcal{K}}$ es un divisor de P^α . Puesto que toda extensión cíclica \mathcal{K}/K de grado p^n tal que $K \subseteq \mathcal{K} \subseteq K(\Lambda_{P^\alpha})$ satisface estas condiciones, tenemos que $v_n(\alpha) \leq t_n(\alpha)$. Si probamos que $t_n(\alpha) \leq v_n(\alpha)$ entonces toda extensión satisfaciendo la ecuación (12.5) está contenida en una extensión ciclotómica y por ende se sigue el Teorema 12.2.1.

En resumen, para probar el Teorema 12.2.1, es suficiente probar

$$t_n(\alpha) \leq v_n(\alpha) \quad \text{para toda } n, \alpha \in \mathbb{N}. \quad (12.6)$$

Demostración de (12.6)

Probaremos ahora por inducción en n la ecuación (12.6) y como consecuencia obtenmos el Teorema 12.2.1. Primero calcularemos $v_n(\alpha)$ para todas $n, \alpha \in \mathbb{N}$.

Proposición 12.2.11. *El número $v_n(\alpha)$ de grupos cíclicos de orden p^n contenidos en $(R_T/(P^\alpha))^*$ es*

$$v_n(\alpha) = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^n} \rceil)} - q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)} = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)} (q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1)}{p^{n-1}(p-1)},$$

donde $\lceil x \rceil$ denota la función techo, esto es, $\lceil x \rceil$ denota al entero más pequeño tal que es mayor o igual a x .

Demostración.

Sea $P \in R_T^+$ y $\alpha \in \mathbb{N}$ con $\text{gr } P = d$. Primero calculamos cuantas extensiones cíclicas de grado p^n están contenidas en $k(\Lambda_{P^\alpha})$. Puesto que \mathfrak{p}_∞ es moderadamente ramificada en $k(\Lambda_{P^\alpha})$, si \mathcal{K}/K es una extensión cíclica de grado p^n , \mathfrak{p}_∞ se descompone totalmente en \mathcal{K}/K ([70, Theorem 12.4.6]). Tenemos $\text{Gal}(k(\Lambda_{P^\alpha})/K) \cong (R_T/(P^\alpha))^*$ y la sucesión exacta

$$0 \longrightarrow D_{P, P^\alpha} \longrightarrow (R_T/(P^\alpha))^* \xrightarrow{\varphi} (R_T/(P))^* \longrightarrow 0, \quad (12.7)$$

donde

$$\begin{aligned} \varphi: (R_T/(P^\alpha))^* &\longrightarrow (R_T/(P))^* \\ A \bmod P^\alpha &\longmapsto A \bmod P \end{aligned}$$

y $D_{P,P^\alpha} = \text{núc } \varphi = \{N \text{ mód } P^\alpha \mid N \equiv 1 \text{ mód } P\}$. Podemos considerar, sin peligro alguno, que $D_{P,P^\alpha} = \{1 + hP \mid h \in R_T, \text{gr } h < \text{gr } P^\alpha = d\alpha\}$.

Tenemos que $(R_T/(P^\alpha))^* \cong (R_T/(P))^* \times D_{P,P^\alpha}$ y que $(R_T/(P))^* \cong C_{q^d-1}$. En primer lugar calculamos cuantos elementos de orden p^n existen en $(R_T/(P^\alpha))^*$. Estos elementos pertenecen a D_{P,P^α} . Sea $A = 1 + hP \in D_{P,P^\alpha}$ de orden p^n . Escribimos $h = gP^\gamma$ con $g \in R_T$, $\text{mcd}(g, P) = 1$ y $\gamma \geq 0$. Tenemos $A = 1 + gP^{1+\gamma}$. Puesto que A es de orden p^n , se sigue que

$$A^{p^n} = 1 + g^{p^n} P^{p^n(1+\gamma)} \equiv 1 \text{ mód } P^\alpha \quad (12.8)$$

y

$$A^{p^{n-1}} = 1 + g^{p^{n-1}} P^{p^{n-1}(1+\gamma)} \not\equiv 1 \text{ mód } P^\alpha. \quad (12.9)$$

De (12.8) y (12.9) se obtiene

$$p^{n-1}(1+\gamma) < \alpha \leq p^n(1+\gamma) \quad (12.10)$$

y (12.10) es equivalente a

$$\left\lceil \frac{\alpha}{p^n} \right\rceil - 1 \leq \gamma < \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 1. \quad (12.11)$$

Notemos que para la existencia de al menos un elemento de orden p^n es necesario que $\alpha > p^{n-1}$.

Ahora para cada γ que satisface (12.10) tenemos $\text{mcd}(g, P) = 1$ y $\text{gr } g + d(1+\gamma) < d\alpha$, esto es, $\text{gr } g < d(\alpha - \gamma - 1)$. Luego, existen $\Phi(P^{\alpha-\gamma-1})$ tales g 's, donde para cualquier $N \in R_T$, $\Phi(N) := |(R_T/(N))^*|$.

Por lo tanto el número de elementos de orden p^n en D_{P,P^α} es

$$\sum_{\gamma=\left\lceil \frac{\alpha}{p^n} \right\rceil - 1}^{\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 2} \Phi(P^{\alpha-\gamma-1}) = \sum_{\gamma'=\alpha-\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil + 1}^{\alpha-\left\lceil \frac{\alpha}{p^n} \right\rceil} \Phi(P^{\gamma'}). \quad (12.12)$$

Notemos que para cualquier $1 \leq r \leq s$ tenemos

$$\begin{aligned} \sum_{i=r}^s \Phi(P^i) &= \sum_{i=r}^s q^{d(i-1)}(q^d - 1) = (q^d - 1)q^{d(r-1)} \sum_{j=0}^{s-r} q^{dj} \\ &= (q^d - 1)q^{d(r-1)} \frac{q^{d(s-r+1)} - 1}{q^d - 1} = q^{ds} - q^{d(r-1)}. \end{aligned}$$

Luego, (12.12) es igual a

$$q^{d(\alpha-\left\lceil \frac{\alpha}{p^n} \right\rceil)} - q^{d(\alpha-\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil)} = q^{d(\alpha-\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil)} (q^{d(\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - \left\lceil \frac{\alpha}{p^n} \right\rceil)} - 1).$$

Puesto que cada grupo cíclico de orden p^n tiene $\varphi(p^n) = p^{n-1}(p-1)$ generadores, se sigue el resultado. \square

Notemos que si \mathcal{K}/K es cualquier campo contenido en $K(\Lambda_{P^\alpha})$ entonces es conductor $\mathfrak{F}_{\mathcal{K}}$ de \mathcal{K} es un divisor de P^α (Lema 11.8.24).

Ahora calculamos el número de extensiones cíclicas \mathcal{K}/K de grado p tales que P es el único primo ramificado (es completamente ramificado), \mathfrak{p}_∞ se descompone en \mathcal{K}/K y $\mathfrak{F}_{\mathcal{K}} \mid P^\alpha$.

Proposición 12.2.12. *Toda extensión cíclica \mathcal{K}/K de grado p tal que P es el único primo ramificado, \mathfrak{p}_∞ se descompone en \mathcal{K}/K y $\mathfrak{F}_{\mathcal{K}} \mid P^\alpha$ está contenido en $k(\Lambda_{P^\alpha})$.*

Demostración. De la Teoría de Artin–Schreier (ver (12.2)) y Proposición 12.2.5 se tiene que \mathcal{K} satisface $\mathcal{K} = K(y)$ con la ecuación de Artin–Schreier de y normalizada como prescrita por Hasse ([20] y Observación 11.8.28). Por lo tanto

$$y^p - y = \frac{Q}{P^\lambda},$$

donde $P \in R_T^+$, $Q \in R_T$, $\text{mcd}(P, Q) = 1$, $\lambda > 0$, $p \nmid \lambda$, $\text{gr } Q < \text{gr } P^\lambda$. Ahora el conductor $\mathfrak{F}_{\mathcal{K}}$ satisface $\mathfrak{F}_{\mathcal{K}} = P^{\lambda+1}$ así que $\lambda \leq \alpha - 1$.

Tenemos que si $\mathcal{K} = K(z)$ con $z^p - z = a$ entonces existen $j \in \mathbb{F}_p^*$ y $c \in K$ tales que $z = jy + c$ y $a = j \frac{Q}{P^\lambda} + \wp(c)$ donde $\wp(c) := c^p - c$. Si a está dado en forma normal entonces $c = \frac{h}{P^{\gamma_0}}$ con $p\gamma_0 \leq \lambda$ (de hecho, $p\gamma_0 < \lambda$ puesto que $\text{mcd}(\lambda, p) = 1$) y $\text{gr } h < \text{gr } P^{\gamma_0}$ o $h = 0$. Sea $\gamma_0 := \lfloor \frac{\alpha-1}{p} \rfloor$. Entonces cualquier tal c puede ser escrito como $c = \frac{hP^{\gamma_0-\gamma}}{P^{\gamma_0}}$. Por lo tanto $c \in \mathcal{G} := \left\{ \frac{h}{P^{\gamma_0}} \mid h \in R_T, \text{gr } h < \text{gr } P^{\gamma_0} = d\gamma_0 \text{ o } h = 0 \right\}$.

Si $c \in \mathcal{G}$ y $j \in \{1, 2, \dots, p-1\}$ tenemos

$$\begin{aligned} a &= j \frac{Q}{P^\lambda} + \wp(c) = j \frac{Q}{P^\lambda} + \frac{h^p}{P^{p\gamma_0}} + \frac{h}{P^{\gamma_0}} \\ &= \frac{jQ + P^{\lambda-p\gamma_0}h + P^{\lambda-\gamma_0}h}{P^\lambda} = \frac{Q_1}{P^\lambda}, \end{aligned}$$

con $\text{gr } Q_1 < \text{gr } P^\lambda$. Puesto que $\lambda - p\gamma_0 > 0$ y $\lambda - \gamma_0 > 0$, tenemos $\text{mcd}(Q_1, P) = 1$. Por lo tanto a está en forma normal.

Se sigue que el mismo campo tiene $|\mathbb{F}_p^*||\wp(\mathcal{G})|$ representaciones diferentes, todas ellas en forma normal. Ahora \mathcal{G} y $\wp(\mathcal{G})$ son grupos aditivos y $\wp: \mathcal{G} \rightarrow \wp(\mathcal{G})$ es un epimorfismo de grupos con núcleo $\text{nuc } \wp = \mathcal{G} \cap \{c \mid \wp(c) = c^p - c = 0\} = \mathcal{G} \cap \mathbb{F}_p = \{0\}$. Tenemos $|\wp(\mathcal{G})| = |\mathcal{G}| = |R_T/(P^{\gamma_0})| = q^{d\gamma_0}$.

De la discusión anterior se desprende que el número de extensiones cíclicas diferentes \mathcal{K}/K de grado p tales que el conductor de \mathcal{K} es $\mathfrak{F}_{\mathcal{K}} = P^{\lambda+1}$ es igual a

$$\frac{\Phi(P^\lambda)}{|\mathbb{F}_p^*||\wp(\mathcal{G})|} = \frac{q^{d(\lambda-1)}(q^d-1)}{(p-1)q^{d\gamma_0}} = \frac{q^{d(\lambda-\lfloor \frac{\lambda}{p} \rfloor-1)}(q^d-1)}{p-1} = \frac{1}{p-1} \Phi(P^{\lambda-\lfloor \frac{\lambda}{p} \rfloor}). \quad (12.13)$$

Por lo tanto, el número de extensiones cíclicas \mathcal{K}/K de grado p tal que el conductor de \mathcal{K} es $\mathfrak{F}_{\mathcal{K}}$ es un divisor de P^α está dada por $\frac{w(\alpha)}{p-1}$ donde

$$w(\alpha) = \sum_{\substack{\lambda=1 \\ \text{mcd}(\lambda, p)=1}}^{\alpha-1} \Phi(P^{\lambda - [\frac{\lambda}{p}]}). \quad (12.14)$$

Para calcular $w(\alpha)$ escribamos $\alpha - 1 = pt_0 + r_0$ con $t_0 \geq 0$ y $0 \leq r_0 \leq p-1$. Ahora $\{\lambda \mid 1 \leq \lambda \leq \alpha - 1, \text{mcm}(\lambda, p) = 1\} = \mathcal{A} \cup \mathcal{B}$ donde

$$\mathcal{A} = \{pt + r \mid 0 \leq t \leq t_0 - 1, 1 \leq r \leq p-1\} \quad \text{y} \quad \mathcal{B} = \{pt_0 + r \mid 1 \leq r \leq r_0\}.$$

Entonces

$$w(\alpha) = \sum_{\lambda \in \mathcal{A}} \Phi(P^{\lambda - [\frac{\lambda}{p}]}) + \sum_{\lambda \in \mathcal{B}} \Phi(P^{\lambda - [\frac{\lambda}{p}]})$$

donde entendemos que si un conjunto, \mathcal{A} o \mathcal{B} es vacío, la suma respectiva es 0.

Entonces

$$\begin{aligned} w(\alpha) &= \sum_{\substack{0 \leq t \leq t_0 - 1 \\ 1 \leq r \leq p-1}} q^{d(pt+r-t-1)}(q^d - 1) + \sum_{r=1}^{r_0} (q^{d(pt_0+r-t_0-1)})(q^d - 1) \\ &= (q^d - 1) \left(\sum_{t=0}^{t_0-1} q^{d(p-1)t} \right) \left(\sum_{r=1}^{p-1} q^{d(r-1)} \right) + (q^d - 1) q^{d(p-1)t_0} \sum_{r=1}^{r_0} q^{d(r-1)} \\ &= (q^d - 1) \frac{q^{d(p-1)t_0} - 1}{q^{d(p-1)} - 1} \frac{q^{d(p-1)} - 1}{q^d - 1} + (q^d - 1) q^{d(p-1)t_0} \frac{q^{dr_0} - 1}{q^d - 1} \\ &= q^{d((p-1)t_0+r_0)} - 1 = q^{d(pt_0+r_0-t_0)} - 1 = q^{d(\alpha-1 - [\frac{\alpha-1}{p}])} - 1. \end{aligned} \quad (12.15)$$

Entonces, el número de extensiones cíclicas \mathcal{K}/K de grado p tales que P es el único primo ramificado, $\mathfrak{F}_{\mathcal{K}} \mid P^\alpha$ y \mathfrak{p}_∞ se descompone, es

$$\frac{w(\alpha)}{p-1} = \frac{q^{d(\alpha-1 - [\frac{\alpha-1}{p}])} - 1}{p-1}. \quad (12.16)$$

Para finalizar la demostración de la Proposición 12.2.12 necesitamos el siguiente

Lemma 12.2.13. *Para cualquier $\alpha \in \mathbb{Z}$ y $s \in \mathbb{N}$ se tiene*

$$(I) \quad \left[\frac{[\frac{\alpha}{p^s}]}{p} \right] = \left[\frac{\alpha}{p^{s+1}} \right].$$

$$(II) \left\lfloor \frac{\alpha}{p^s} \right\rfloor = \left\lfloor \frac{\alpha - 1}{p^s} \right\rfloor + 1.$$

Demostración. Para (I), notemos que el caso $s = 0$ es claro. Pongamos $\alpha = tp^{s+1} + r$ con $0 \leq r \leq p^{s+1} - 1$. Sea $r = lp^s + r'$ con $0 \leq r' \leq p^s - 1$. Notemos que $0 \leq l \leq p - 1$. Por lo tanto $\alpha = tp^{s+1} + lp^s + r'$, $0 \leq r' \leq p^s - 1$

y $0 \leq l \leq p - 1$. Luego $\left\lfloor \frac{\alpha}{p^s} \right\rfloor = tp + l$, y $\frac{\left\lfloor \frac{\alpha}{p^s} \right\rfloor}{p} = t + \frac{l}{p}$, $0 \leq l \leq p - 1$.

$$\text{Así } \left\lfloor \frac{\left\lfloor \frac{\alpha}{p^s} \right\rfloor}{p} \right\rfloor = t = \left\lfloor \frac{\alpha}{p^{s+1}} \right\rfloor.$$

Para (II), escribamos $\alpha = p^s t + r$ con $0 \leq r \leq p^s - 1$. Si $p^s \mid \alpha$ entonces $r = 0$ y $\left\lfloor \frac{\alpha}{p^s} \right\rfloor = t$, $\left\lfloor \frac{\alpha - 1}{p^s} \right\rfloor = \left\lfloor \frac{p^s t - 1}{p^s} \right\rfloor = \left\lfloor t - \frac{1}{p^s} \right\rfloor = t - 1 = \left\lfloor \frac{\alpha}{p^s} \right\rfloor - 1$.

Si $p^s \nmid \alpha$, entonces $1 \leq r \leq p^s - 1$ y $\alpha - 1 = p^s t + (r - 1)$ con $0 \leq r - 1 \leq p^s - 2$. Por tanto $\left\lfloor \frac{\alpha}{p^s} \right\rfloor = \left\lfloor t + \frac{r}{p^s} \right\rfloor = t + 1$ y $\left\lfloor \frac{\alpha - 1}{p^s} \right\rfloor = \left\lfloor t + \frac{r - 1}{p^s} \right\rfloor = t = \left\lfloor \frac{\alpha}{p^s} \right\rfloor - 1$. \square

Del Lema 12.2.13 (I) obtenemos que (12.16) es igual a

$$\frac{w(\alpha)}{p - 1} = \frac{q^{d(\alpha - 1 - (\left\lfloor \frac{\alpha}{p} \right\rfloor - 1))} - 1}{p - 1} = \frac{q^{d(\alpha - \left\lfloor \frac{\alpha}{p} \right\rfloor)} - 1}{p - 1} = v_1(\alpha). \quad (12.17)$$

Como consecuencia de (12.17), tenemos la Proposición 12.2.12. \square

La Proposición 12.2.12 prueba (12.6) para $n = 1$ y toda $\alpha \in \mathbb{N}$.

Ahora consideremos una extensión cíclica \mathcal{K}_n/K de grado p^n tal que P es el único primo ramificado, es completamente ramificado, \mathfrak{p}_∞ se descompone completamente en \mathcal{K}_n/K y $\mathfrak{F}_{\mathcal{K}} \mid P^\alpha$. Queremos probar que $\mathcal{K}_n \subseteq k(\Lambda_{P^\alpha})$. Esto será probado por inducción en n . El caso $n = 1$ es la Proposición 12.2.12. Suponemos que toda extensión cíclica \mathcal{K}_{n-1} de grado p^{n-1} , $n \geq 2$ tal que P es el único primo ramificado, \mathfrak{p}_∞ se descompone completamente en \mathcal{K}_{n-1}/K y tal que $\mathfrak{F}_{\mathcal{K}_{n-1}} \mid P^\delta$ está contenida en $k(\Lambda_{P^\delta})$ donde $\delta \in \mathbb{N}$.

Sea \mathcal{K}_n cualquier extensión cíclica de grado p^n tal que P es el único primo ramificado y es totalmente ramificado, \mathfrak{p}_∞ se descompone totalmente en \mathcal{K}_n/K y $\mathfrak{F}_{\mathcal{K}_n} \mid P^\alpha$. Sea \mathcal{K}_{n-1} el subcampo de \mathcal{K}_n de grado p^{n-1} . Ahora consideremos \mathcal{K}_n/K generado por el vector de Witt $\beta = (\beta_1, \dots, \beta_{n-1}, \beta_n)$, esto es, $\wp(\mathbf{y}) = \mathbf{y}^p \cdot \mathbf{y} = \beta$, y suponemos que β está en su forma normal descrita por Schmid (ver Observación 11.8.28, [64, 65]). Entonces \mathcal{K}_{n-1}/K está dado por el vector de Witt $\beta' = (\beta_1, \dots, \beta_{n-1})$.

Sea $\lambda := (\lambda_1, \dots, \lambda_{n-1}, \lambda_n)$ el vector de los parámetros de Schmid, esto es, donde cada β_i está dado por

$$\beta_i = \frac{Q_i}{P^{\lambda_i}}, \text{ donde } Q_i = 0 \text{ (esto es, } \beta_i = 0) \text{ y } \lambda_i := 0 \text{ o}$$

$$\text{mcd}(Q_i, P) = 1, \text{ gr } Q_i < \text{gr } P^{\lambda_i}, \lambda_i > 0 \text{ y } \text{mcd}(\lambda_i, p) = 1.$$

Ahora, puesto que P es totalmente ramificado, se tiene $\lambda_1 > 0$.

Ahora calculamos cuantas extensiones $\mathcal{K}_n/\mathcal{K}_{n-1}$ diferentes pueden ser construidas por medio de β_n .

Lema 12.2.14. *Para un campo fijo \mathcal{K}_{n-1} , el número de campos diferentes \mathcal{K}_n es menor o igual a*

$$\frac{1 + w(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}. \quad (12.18)$$

Demostración. Para $\beta_n \neq 0$, cada ecuación en forma normal está dada por

$$y_n^p - y_n = z_{n-1} + \beta_n, \quad (12.19)$$

donde z_{n-1} es el elemento en \mathcal{K}_{n-1} obtenido por la generación de Witt de \mathcal{K}_{n-1} del vector β' (ver [64, Page 109]). De hecho z_{n-1} está dado, formalmente, por

$$z_{n-1} = \sum_{i=1}^{n-1} \frac{1}{p^{n-i}} [y_i^{p^{n-i}} + \beta_i^{p^{n-i}} - (y_i + \beta_i + z_{i-1})^{p^{n-i}}],$$

con $z_0 = 0$.

Como en el caso $n = 1$ tenemos que existen $\Phi(P^{\lambda_n})$ extensiones para los diferentes β_n con $\lambda_n > 0$. El número de elementos β_n diferentes que nos dan el mismo campo \mathcal{K}_n con el cambio $y_n \rightarrow y_n + c$, $c \in \mathcal{G}_{\lambda_n} := \{ \frac{h}{p^{\gamma_0}} \mid h \in R_T, \text{gr } h < \text{gr } P^{\gamma_0} = d\gamma_0 \text{ o } h = 0 \}$ donde $\gamma_n = \left\lfloor \frac{\lambda_n}{p} \right\rfloor$, obtenemos $\beta_n \rightarrow \beta_n + \wp(c)$ está también en forma normal. Por tanto, el número de elementos β_n que nos dan el mismo campo \mathcal{K}_n con este cambio de variable es $q^{d(\lceil \frac{\lambda_n}{p} \rceil)}$. Por lo tanto obtenemos a lo más $\Phi(P^{\lambda_n - \lceil \frac{\lambda_n}{p} \rceil})$ posibles campos \mathcal{K}_n para cada $\lambda_n > 0$ (ver (12.16)). Más precisamente, si para cada β_n con $\lambda_n > 0$ definimos $\overline{\beta_n} := \{ \beta_n + \wp(c) \mid c \in \mathcal{G}_{\lambda_n} \}$, entonces cada elemento de $\overline{\beta_n}$ nos da el mismo campo \mathcal{K}_n .

Sea v_P la valuación en P y

$$\mathcal{A}_{\lambda_n} := \{ \overline{\beta_n} \mid v_P(\beta_n) = -\lambda_n \},$$

$$\mathcal{A} := \bigcup_{\substack{\lambda_n=1 \\ \text{mcd}(\lambda_n, p)=1}}^{\alpha-1} \mathcal{A}_{\lambda_n}.$$

Entonces cada campo \mathcal{K}_n está dado por $\beta_n = 0$ o $\overline{\beta_n} \in \mathcal{A}$. De (12.15) Tenemos que el número de campos \mathcal{K}_n conteniendo un campo fijo \mathcal{K}_{n-1} que obtuvimos en (12.19) es menor o igual a

$$1 + |\mathcal{A}| = 1 + w(\alpha) = q^{d(\alpha - 1 - \lceil \frac{\alpha-1}{p} \rceil)} = q^{d(\alpha - 1 - \lceil \frac{\alpha}{p} \rceil + 1)} = q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}. \quad (12.20)$$

Ahora con la substitución $y_n \rightarrow y_n + jy_1$, $j = 0, 1, \dots, p-1$, en (12.19) obtenemos

$$(y_n + jy_1)^p - (y_n + jy_1) = y_n^p - y_n + j(y_1^p - y_1) = z_{n-1} + \beta_n + j\beta_1.$$

Por lo tanto, cada una de las extensiones obtenidas en (12.19) se repite al menos p veces, esto es, para cada β_n , obtenemos la misma extensión con $\beta_n, \beta_n + \beta_1, \dots, \beta_n + (p-1)\beta_1$. Probaremos que diferentes $\beta_n + j\beta_1$ corresponden a elementos diferentes de $\{0\} \cup \mathcal{A}$.

Fijemos β_n . Modificamos cada $\beta_n + j\beta_1$ en su forma normal: $\beta_n + j\beta_1 + \wp(c_{\beta_n, j})$ para alguna $c_{\beta_n, j} \in K$. De hecho $\beta_n + j\beta_1$ está siempre en forma normal con la posible excepción de $\lambda_n = \lambda_1$ y aún en este caso esto sucede para a lo más un índice $j \in \{0, 1, \dots, p-1\}$: si $\lambda_n \neq \lambda_1$,

$$v_P(\beta_n + j\beta_1) = \begin{cases} -\lambda_n & \text{si } j = 0 \\ -\max\{-\lambda_n, -\lambda_1\} & \text{si } j \neq 0 \end{cases}.$$

Cuando $\lambda_n = \lambda_1$ y si $v_P(\lambda_n + j\lambda_1) = u > -\lambda_n = -\lambda_1$ y $p \nmid u$, entonces para $i \neq j$, $v_P(\beta_n + i\beta_1) = v_P(\beta_n + j\beta_1 + (i-j)\beta_1) = -\lambda_n = -\lambda_1$. En otras palabras $c_{\beta_n, j} = 0$ con muy pocas excepciones.

Cada $\mu = \beta_n + j\beta_1 + \wp(c_{\beta_n, j})$, $j = 0, 1, \dots, p-1$ satisface que o bien $\mu = 0$ o $\bar{\mu} \in \mathcal{A}$. Veremos que todos estos elementos nos dan elementos diferentes de $\{0\} \cup \mathcal{A}$.

Si $\beta_n = 0$, entonces para $j \neq 0$, $v_P(j\beta_1) = -\lambda_1$, de tal forma que $\overline{j\beta_1} \in \mathcal{A}$. Ahora si $\overline{j\beta_1} = \overline{i\beta_1}$, entonces

$$j\beta_1 = \beta'_n + \wp(c_1) \quad \text{y} \quad i\beta_1 = \beta'_n + \wp(c_2)$$

para alguna $\beta'_n \neq 0$ y algunas $c_1, c_2 \in \mathcal{G}_{\lambda_1}$. Se sigue que $(j-i)\beta_1 = \wp(c_2 - c_1) \in \wp(K)$. Esto no es posible por la elección de β_1 a menos que $j = i$.

Sea $\beta_n \neq 0$. El caso $\beta_n + j\beta_1 = 0$ para alguna $j \in \{0, 1, \dots, p-1\}$ ha sido ya considerada en el primer caso. Por tanto consideramos el caso $\beta_n + j\beta_1 + \wp(c_{\beta_n, j}) \neq 0$ para toda j . Si para algunas $i, j \in \{0, 1, \dots, p-1\}$ tenemos $\overline{\beta_n + j\beta_1 + \wp(c_{\beta_n, j})} = \overline{\beta_n + i\beta_1 + \wp(c_{\beta_n, i})}$ entonces existen β'_n y $c_1, c_2 \in K$ tales que

$$\beta_n + j\beta_1 + \wp(c_{\beta_n, j}) = \beta'_n + \wp(c_1) \quad \text{y} \quad \beta_n + i\beta_1 + \wp(c_{\beta_n, i}) = \beta'_n + \wp(c_2).$$

Se sigue que $(j-i)\beta_1 = \wp(c_1 - c_2 + c_{\beta_n, i} - c_{\beta_n, j}) \in \wp(K)$ de tal forma que $i = j$.

Por tanto cada campo \mathcal{K}_n es representado por al menos p elementos diferentes de $\{0\} \cup \mathcal{A}$. El resultado se sigue. \square

Ahora bien, de acuerdo con Schmid (Teorema 11.8.29), el conductor de \mathcal{K}_n es P^{M_n+1} donde $M_n = \max\{pM_{n-1}, \lambda_n\}$ y $P^{M_{n-1}+1}$ es el conductor de \mathcal{K}_{n-1} . Puesto que $\mathfrak{F}_{\mathcal{K}_n} \mid P^\alpha$, se tiene $M_n \leq \alpha - 1$. Por lo tanto $pM_{n-1} \leq \alpha - 1$ y $\lambda_n \leq \alpha - 1$. Luego $\mathfrak{F}_{\mathcal{K}_{n-1}} \mid P^\delta$ con $\delta = \left\lfloor \frac{\alpha - 1}{p} \right\rfloor + 1$.

Proposición 12.2.15. *Se tiene*

$$\frac{v_n(\alpha)}{v_{n-1}(\delta)} = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}}{p},$$

donde $\delta = \left\lceil \frac{\alpha - 1}{p} \right\rceil + 1$.

Demostración. De la Proposición 12.2.11 obtenemos

$$\begin{aligned} v_n(\alpha) &= \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)} (q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1)}{p^{n-1}(p-1)} \\ &= \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)} (q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1), \end{aligned}$$

y

$$\begin{aligned} v_{n-1}(\delta) &= \frac{q^{d(\delta - \lceil \frac{\delta}{p^{n-2}} \rceil)} (q^{d(\lceil \frac{\delta}{p^{n-2}} \rceil - \lceil \frac{\delta}{p^{n-1}} \rceil)} - 1)}{p^{n-2}(p-1)} \\ &= \frac{q^{d(\delta - \lceil \frac{\delta}{p^{n-2}} \rceil)}}{p^{n-2}(p-1)} (q^{d(\lceil \frac{\delta}{p^{n-2}} \rceil - \lceil \frac{\delta}{p^{n-1}} \rceil)} - 1). \end{aligned}$$

Ahora del Lema 12.2.13 obtenemos

$$\begin{aligned} \left\lceil \frac{\delta}{p^{n-2}} \right\rceil - \left\lceil \frac{\delta}{p^{n-1}} \right\rceil &= \left(\left\lceil \frac{\delta - 1}{p^{n-2}} \right\rceil + 1 \right) - \left(\left\lceil \frac{\delta - 1}{p^{n-1}} \right\rceil + 1 \right) \\ &= \left\lceil \frac{\delta - 1}{p^{n-2}} \right\rceil - \left\lceil \frac{\delta - 1}{p^{n-1}} \right\rceil = \left\lceil \frac{\lceil \frac{\alpha - 1}{p} \rceil}{p^{n-2}} \right\rceil - \left\lceil \frac{\lceil \frac{\alpha - 1}{p} \rceil}{p^{n-1}} \right\rceil \\ &= \left\lceil \frac{\alpha - 1}{p^{n-1}} \right\rceil - \left\lceil \frac{\alpha - 1}{p^n} \right\rceil = \left(\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 1 \right) - \left(\left\lceil \frac{\alpha}{p^n} \right\rceil - 1 \right) \\ &= \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - \left\lceil \frac{\alpha}{p^n} \right\rceil, \\ \delta - \left\lceil \frac{\delta}{p^{n-2}} \right\rceil &= \left(\left\lceil \frac{\alpha - 1}{p} \right\rceil + 1 \right) - \left(\left\lceil \frac{\delta - 1}{p^{n-2}} \right\rceil + 1 \right) \\ &= \left\lceil \frac{\alpha - 1}{p} \right\rceil - \left\lceil \frac{\delta - 1}{p^{n-2}} \right\rceil = \left\lceil \frac{\alpha - 1}{p} \right\rceil - \left\lceil \frac{\lceil \frac{\alpha - 1}{p} \rceil}{p^{n-2}} \right\rceil \\ &= \left\lceil \frac{\alpha - 1}{p} \right\rceil - \left\lceil \frac{\alpha - 1}{p^{n-1}} \right\rceil. \end{aligned}$$

Por tanto

$$v_{n-1}(\delta) = \frac{q^{d(\lceil \frac{\alpha-1}{p} \rceil - \lceil \frac{\alpha-1}{p^{n-1}} \rceil)}}{p^{n-2}(p-1)} \left(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1 \right).$$

Así, por el Lema 12.2.13,

$$\begin{aligned} \frac{v_n(\alpha)}{v_{n-1}(\delta)} &= \frac{\frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)} \left(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1 \right)}{\frac{q^{d(\lceil \frac{\alpha-1}{p} \rceil - \lceil \frac{\alpha-1}{p^{n-1}} \rceil)}}{p^{n-2}(p-1)} \left(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1 \right)} \\ &= \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil) - [\frac{\alpha-1}{p}] + [\frac{\alpha-1}{p^{n-1}}]} \\ &= \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil) - (\lceil \frac{\alpha}{p} \rceil - 1) + (\lceil \frac{\alpha}{p^{n-1}} \rceil - 1)} \\ &= \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}. \end{aligned}$$

Esto prueba el resultado. \square

De aquí, de la Proposición 12.2.15, Lema 12.2.14 (12.18) y puesto que por hipótesis de inducción tenemos $t_{n-1}(\delta) = v_{n-1}(\delta)$, obtenemos

$$t_n(\alpha) \leq t_{n-1}(\delta) \left(\frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)} \right) = v_{n-1}(\delta) \left(\frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)} \right) = v_n(\alpha).$$

Esto prueba (12.6) y el Teorema 12.2.1.

Prueba alternativa de (12.6)

Mantenemos la misma notación de las subsecciones previas. Sea \mathcal{K}/K una extensión satisfaciendo las condiciones de (12.5) y con el conductor un divisor de P^α . Tenemos que $\mathfrak{F}_{\mathcal{K}} = P^{M_n+1}$ donde

$$M_n = \max\{p^{n-1}\lambda_1, p^{n-2}\lambda_2, \dots, p\lambda_{n-1}, \lambda_n\}$$

ver Teorema 11.8.29. Por lo tanto

$$\mathfrak{F}_{\mathcal{K}} \mid P^\alpha \iff M_n + 1 \leq \alpha \iff p^{n-i}\lambda_i \leq \alpha - 1, \quad i = 1, \dots, n.$$

Entonces $\lambda_i \leq \left\lceil \frac{\alpha-1}{p^{n-i}} \right\rceil$. Estas condiciones proporcionan todas las extensiones cíclicas de grado p^n donde $P \in R_T^+$ es el único primo ramificado, es totalmente ramificado, \mathfrak{p}_∞ se decompone totalmente y su conductor divide a P^α . Ahora estimamos el número de diferentes formas para generar \mathcal{K} .

Let $\mathcal{K} = K(\mathbf{y})$. Primero notemos que con el cambio de variable y_i por $y_i + c_i$ para cada i , $c_i \in K$ obtenemos el mismo campo. Para estas nuevas formas de generar \mathcal{K} que a su vez cumpla (12.5), debemos tener:

- (I) Si $\lambda_i = 0$, $c_i = 0$.
 (II) Si $\lambda_i > 0$, entonces $c_i \in \left\{ \frac{h}{p^{\gamma_i}} \mid h \in R_T, \text{gr } h < \text{gr } P^{\gamma_i} = d\gamma_i \text{ o } h = 0 \right\}$, donde $\gamma_i = \left\lfloor \frac{\lambda_i}{p} \right\rfloor$. Por lo tanto tenemos a lo más $\Phi(P^{\lambda_i - \left\lfloor \frac{\lambda_i}{p} \right\rfloor})$ extensiones para este λ_i (ver (12.13)). Puesto que $1 \leq \lambda_i \leq \left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor$ y $\text{mcd}(\lambda_i, p) = 1$, si definimos $\delta_i := \left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor + 1$, de (12.14) y de (12.15) obtenemos que debemos tener a lo más

$$w(\delta_i) = \sum_{\substack{\lambda_i=1 \\ \text{mcm}(\lambda_i, p)=1}}^{\delta_i-1} \Phi(P^{\lambda_i - \left\lfloor \frac{\lambda_i}{p} \right\rfloor}) = q^{d(\delta_i-1 - \left\lfloor \frac{\delta_i-1}{p} \right\rfloor)} - 1 \quad (12.21)$$

expresiones diferentes para todos los posibles $\lambda_i > 0$.
 Ahora del Lema 12.2.13 tenemos

$$\delta_i - 1 - \left\lfloor \frac{\delta_i - 1}{p} \right\rfloor = \left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor - \left\lfloor \frac{\left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor - \left\lfloor \frac{\alpha - 1}{p^{n-i+1}} \right\rfloor.$$

Por tanto

$$w(\delta_i) = q^{d\left(\left\lfloor \frac{\alpha-1}{p^{n-i}} \right\rfloor - \left\lfloor \frac{\alpha-1}{p^{n-i+1}} \right\rfloor\right)} - 1. \quad (12.22)$$

Cuando $\lambda_i = 0$ es permitido tenemos a lo más $w(\delta_i) + 1$ extensiones con parámetro λ_i . Por tanto, puesto que $\lambda_1 > 0$ y $\lambda_i \geq 0$ for $i = 2, \dots, n$, tenemos que el número de extensiones satisfaciendo (12.5) y con conductor un divisor de P^α es a lo más

$$s_n(\alpha) := w(\delta_1) \cdot \prod_{i=2}^n (w(\delta_i) + 1).$$

De (12.21) y de (12.22), obtenemos

$$s_n(\alpha) = \left(q^{d\left(\left\lfloor \frac{\alpha-1}{p^{n-1}} \right\rfloor - \left\lfloor \frac{\alpha-1}{p^n} \right\rfloor\right)} - 1 \right) \cdot \prod_{i=2}^n q^{d\left(\left\lfloor \frac{\alpha-1}{p^{n-i}} \right\rfloor - \left\lfloor \frac{\alpha-1}{p^{n-i+1}} \right\rfloor\right)}.$$

Por lo tanto $\prod_{i=2}^n (w(\delta_i) + 1) = q^{d\mu}$ donde

$$\begin{aligned} \mu &= \sum_{i=2}^n \left(\left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor - \left\lfloor \frac{\alpha - 1}{p^{n-i+1}} \right\rfloor \right) = \sum_{i=2}^n \left\lfloor \frac{\alpha - 1}{p^{n-i}} \right\rfloor - \sum_{j=1}^{n-1} \left\lfloor \frac{\alpha - 1}{p^{n-j}} \right\rfloor \\ &= \left\lfloor \frac{\alpha - 1}{p^{n-n}} \right\rfloor - \left\lfloor \frac{\alpha - 1}{p^{n-1}} \right\rfloor = \alpha - 1 - \left\lfloor \frac{\alpha - 1}{p^{n-1}} \right\rfloor. \end{aligned}$$

Se sigue que

$$\begin{aligned}
 s_n(\alpha) &= \left(q^{d\left(\left[\frac{\alpha-1}{p^{n-1}}\right] - \left[\frac{\alpha-1}{p^n}\right]\right)} - 1 \right) \cdot q^{d\left(\alpha-1 - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)} \\
 &= q^{d\left(\left[\frac{\alpha-1}{p^{n-1}}\right] - \left[\frac{\alpha-1}{p^n}\right] + \alpha-1 - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)} - q^{d\left(\alpha-1 - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)} \\
 &= q^{d\left(\alpha-1 - \left[\frac{\alpha-1}{p^n}\right]\right)} - q^{d\left(\alpha-1 - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)}.
 \end{aligned}$$

Del Lema 12.2.13 (II) obtenemos

$$\alpha - 1 - \left\lfloor \frac{\alpha-1}{p^n} \right\rfloor = \alpha - \left\lfloor \frac{\alpha}{p^n} \right\rfloor \quad \text{y} \quad \alpha - 1 - \left\lfloor \frac{\alpha-1}{p^{n-1}} \right\rfloor = \alpha - \left\lfloor \frac{\alpha}{p^{n-1}} \right\rfloor.$$

Por tanto

$$s_n(\alpha) = q^{\left(\alpha - \left\lfloor \frac{\alpha}{p^n} \right\rfloor\right)} - q^{\left(\alpha - \left\lfloor \frac{\alpha}{p^{n-1}} \right\rfloor\right)} = p^{n-1}(p-1)v_n(\alpha).$$

Finalmente, el cambio de variable $\mathbf{y} \rightarrow \mathbf{j} \dot{\times} \mathbf{y}$ con $\mathbf{j} \in W_n(\mathbb{F}_p)^* \cong (\mathbb{Z}/p^n\mathbb{Z})^*$ da el mismo campo y tenemos $\beta \rightarrow \mathbf{j} \dot{\times} \beta$. Por tanto

$$t_n(\alpha) \leq \frac{s_n(\alpha)}{\varphi(p^n)} = \frac{s_n(\alpha)}{p^n(p-1)} = v_n(\alpha).$$

Esto prueba (12.6) y el Teorema 12.2.1.

12.3. Campo de géneros

Para esta sección usaremos las siguientes notaciones. Sea R_T^+ el conjunto de polinomios mónicos e irreducibles en R_T . Para cualquier campo de funciones \mathcal{K}/\mathbb{F}_q , $\mathcal{K}_m := \mathcal{K}\mathbb{F}_{q^m}$ denota a la extensión de constantes. Para cualquier $m \in \mathbb{N}$, C_m denota un grupo cíclico de orden m .

Para cualquier extensión finita \mathcal{K}/K usaremos el símbolo $S_\infty(\mathcal{K})$ para denotar ya sea un primo o todos los primos en \mathcal{K} sobre \mathfrak{p}_∞ , el divisor de polos de T en K . Recordemos que los primos que se ramifican en $K(\Lambda_N)/K$ son \mathfrak{p}_∞ ($q \neq 2$) y los polinomios $P \in R_T^+$ tales que $P \mid N$, con la excepción de que $q = 2$ y $N \in \{T, T+1, T(T+1)\}$ en cuyo caso $K(\Lambda_N) = K$.

Establecemos L_n como el máximo subcampo de $K(\Lambda_{1/T^n})$ donde \mathfrak{p}_∞ es total y salvajemente ramificado, $n \in \mathbb{N}$. Para cualquier campo F , ${}_nF$ denota la composición FL_n .

La definición de Rosen para un campo de clase de Hilbert relativo de un campo de funciones congruente \mathcal{K} , es la siguiente.

Definición 12.3.1 ([55]). Sea \mathcal{K} un campo de funciones con campo de constantes \mathbb{F}_q . Sea S cualquier conjunto finito no vacío de divisores primos de \mathcal{K} . El *campo de clase de Hilbert de \mathcal{K} relativo a S* , $\mathcal{K}_{H,S}$, es el la máxima extensión abeliana no ramificada de \mathcal{K} donde cada elemento de S se descompone totalmente.

A partir de ahora, para cualquier extensión finita \mathcal{K} de K consideraremos S como el conjunto de divisores primos que dividen a \mathfrak{p}_∞ , el divisor de polos de T en K y escribiremos \mathcal{K}_H en lugar de $\mathcal{K}_{H,S}$.

Definición 12.3.2. Sea \mathcal{K} una extensión geométrica finita de K . El *campo de géneros* $\mathcal{K} \mathfrak{ge}$ de \mathcal{K} es la máxima extensión de \mathcal{K} contenida en \mathcal{K}_H que sea la composición de \mathcal{K} y una extensión abeliana de K . Equivalentemente, $\mathcal{K} \mathfrak{ge} = \mathcal{K} K^*$ donde K^* es la máxima extensión abeliana de K contenida en \mathcal{K}_H .

Cuando \mathcal{K}/K es una extensión abeliana, $\mathcal{K} \mathfrak{ge}$ es la máxima extensión de K contenida en \mathcal{K}_H . El principal objetivo en esta sección es encontrar $\mathcal{K} \mathfrak{ge}$ donde \mathcal{K} es un subcampo de un campo de funciones ciclotómico. En lo que sigue, \mathcal{K} siempre denotará una extensión finita geométrica de K . Primero notamos que tenemos el análogo al resultado de Leopoldt (Teorema 6.4.2).

Proposición 12.3.3. Si $\mathcal{K} \subseteq K(\Lambda_N)$ y el grupo de caracteres asociado a \mathcal{K} es X , entonces la máxima extensión abeliana J de \mathcal{K} no ramificada en ningún primo finito $P \in R_T^+$, contenida en una extensión ciclotómica, es el campo asociado a $Y = \prod_{P \in R_T^+} X_P = \prod_{P|N} X_P$.

Demostración. Análoga a la demostración del Teorema 6.4.2. \square

En este caso \mathfrak{p}_∞ no tiene inercia en J/\mathcal{K} pero bien podría ser ramificado.

Proposición 12.3.4. Si E/K es una extensión abeliana tal que \mathfrak{p}_∞ es moderadamente ramificado, existen $N \in R_T$ y $m \in \mathbb{N}$ tales que $E \subseteq K(\Lambda_N)\mathbb{F}_{q^m}$.

Demostración. Por el Teorema de Kronecker–Weber (Teorema 12.2.1), tenemos $E \subseteq K(\Lambda_N)\mathbb{F}_{q^m} L_n = {}_n K(\Lambda_N)_m$ para algunos $N \in R_T$ y $n, m \in \mathbb{N}$.

Sea $F := K(\Lambda_N)\mathbb{F}_{q^m} = K(\Lambda_N)_m$ y sea V el primer grupo de ramificación de \mathfrak{p}_∞ en FL_n/K . Entonces $R := (FL_n)^V$ es la máxima extensión de K donde \mathfrak{p}_∞ es moderadamente ramificado y como consecuencia tenemos que $S_\infty(R)$ es salvajemente ramificado en FL_n/R . Puesto que \mathfrak{p}_∞ es moderadamente ramificado en E/K , se sigue que $E \subseteq R$. Ahora, \mathfrak{p}_∞ es moderadamente ramificado en F/K y $S_\infty(F)$ es total y salvajemente ramificado en F/K y $S_\infty(F)$ es total y salvajemente ramificado en FL_n/F y FL_n/F es de grado $|V|$. Por tanto $R = F$ y $E \subseteq F$. \square

Proposición 12.3.5. Con las hipótesis de la Proposición 12.3.3, en el caso de que $e_{\mathfrak{p}_\infty}(\mathcal{K}|K) = q - 1$, entonces $\mathcal{K} \mathfrak{ge} = J$.

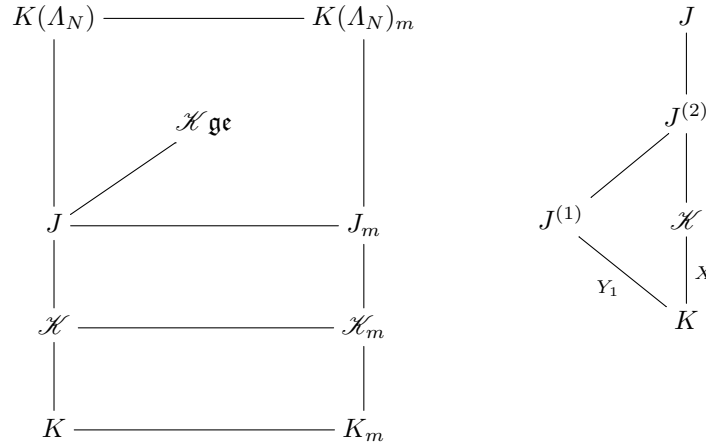
Demostración. Puesto que $e_{\mathfrak{p}_\infty}(J|\mathcal{K}) = \frac{e_{\mathfrak{p}_\infty}(J|K)}{e_{\mathfrak{p}_\infty}(\mathcal{K}|K)} = \frac{q-1}{q-1} = 1$, \mathfrak{p}_∞ se descompone totalmente en J/\mathcal{K} y por tanto $J \subseteq \mathcal{K}\mathfrak{ge}$.

Ahora bien, el campo de constantes de $\mathcal{K}\mathfrak{ge}$ es \mathbb{F}_q (ver [55]) o simplemente si \mathbb{F}_{q^m} es el campo de constantes de $\mathcal{K}\mathfrak{ge}$, $K \subseteq K_m \subseteq \mathcal{K}\mathfrak{ge}$ y \mathfrak{p}_∞ es totalmente inerte en K_m ; puesto que \mathfrak{p}_∞ y $S_\infty(\mathcal{K})$ no tienen inercia en ninguno de \mathcal{K}/K o J/\mathcal{K} , $m = 1$).

Puesto que \mathfrak{p}_∞ se descompone totalmente en $\mathcal{K}\mathfrak{ge}/\mathcal{K}$ y \mathfrak{p}_∞ es moderadamente ramificado en \mathcal{K}/K , por la Proposición 12.3.4 tenemos que $\mathcal{K}\mathfrak{ge} \subseteq K(\Lambda_N)\mathbb{F}_{q^m}$ para algunos $N \in R_T$ y $m \in \mathbb{N}$.

En todas las extensiones K_m/K , $\mathcal{K}_m/\mathcal{K}$, J_m/J , $K(\Lambda_N)_m/K(\Lambda_N)$ los primos infinitos son totalmente inertes ya que todos tienen grado 1 (ver Teorema 9.1.4). En la extensiones \mathcal{K}_m/K_m y \mathcal{K}/K el índice de ramificación de los primos infinitos es $q - 1$, esto es, el máximo posible. Se sigue que en J_m/\mathcal{K}_m , J/\mathcal{K} , $K(\Lambda_N)_m/J_m$, $S_\infty(\mathcal{K}_m)$, $S_\infty(\mathcal{K})$, $S_\infty(J)$ y $S_\infty(J_m)$ son totalmente descompuestos. Finalmente, en $K(\Lambda_N)_m/J$ (y por tanto $K(\Lambda_N)_m/\mathcal{K}\mathfrak{ge}$), $S_\infty(J)$ es no ramificado.

Sea $\mathcal{G} := \text{Gal}(K(\Lambda_N)_m/J)$. Para $S_\infty(J)$ tenemos que en esta extensión el índice de ramificación e , el grado de inercia f y el número de descomposición h son $e = 1$, $f = m$ y $h = \frac{|\mathcal{G}|}{m}$. Por lo tanto el grupo de descomposición \mathfrak{D} de \mathfrak{p}_∞ es de orden m y es cíclico. Debemos tener $\mathfrak{D} = \text{Gal}(K(\Lambda_N)_m/K(\Lambda_N))$ ya que $S_\infty(K(\Lambda_N))$ es totalmente inerte de grado m en $K(\Lambda_N)_m/K(\Lambda_N)$. Puesto que $S_\infty(J)$ tiene grado de inercia 1 en $\mathcal{K}\mathfrak{ge}/J$, se sigue que $\mathcal{K}\mathfrak{ge} \subseteq K(\Lambda_N)$. Por tanto $\mathcal{K}\mathfrak{ge} = J$. \square

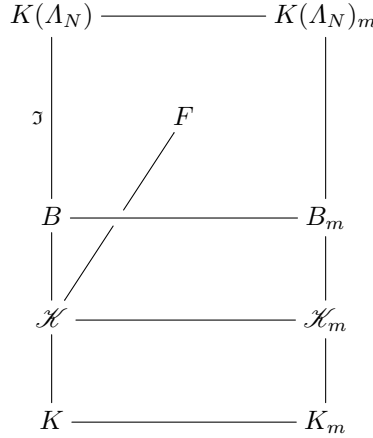


Ahora consideramos el caso general $K \subseteq \mathcal{K} \subseteq K(\Lambda_N)$. Usaremos las notaciones de la Proposición 12.3.3. En este caso $S_\infty(K)$ puede ser ramificado en J/\mathcal{K} . Sea $Y_1 := \{\chi \in Y \mid \chi(a) = 1 \text{ para todo } a \in \mathbb{F}_q^* \subseteq (R_T/(N))^* \cong G_N\}$ y sea $J^{(1)}$ el campo asociado a Y_1 . Entonces $J^{(1)} \subseteq J$ puesto que $Y_1 \subseteq Y$, aunque no necesariamente $J^{(1)} \subseteq \mathcal{K}$ o $\mathcal{K} \subseteq J^{(1)}$. Sea $J^{(2)} := \mathcal{K}J^{(1)}$.

Entonces $J^{(2)}$ es el campo asociado al grupo de caracteres XY_1 . Puesto que \mathfrak{p}_∞ se descompone totalmente en $J^{(1)}/K$, $S_\infty(\mathcal{K})$ se descompone totalmente en $J^{(2)}$. Más aún $S_\infty(J^{(1)})$ es totalmente ramificado en $J/J^{(1)}$. Por tanto $S_\infty(J^{(2)})$ es totalmente ramificado en $J/J^{(2)}$.

Obtenemos que $J^{(2)}/\mathcal{K}$ es una extensión abeliana no ramificada con $J^{(2)} \subseteq K(\Lambda_N)$ y $S_\infty(\mathcal{K})$ se descompone totalmente en $J^{(2)}/\mathcal{K}$. Se sigue que $J^{(2)} = J^{\mathfrak{D}}$ donde \mathfrak{D} es el grupo de descomposición de $S_\infty(J)$ con respecto al grupo $\text{Gal}(J/\mathcal{K})$.

Ahora consideremos cualquier extensión abeliana no ramificada F/\mathcal{K} tal que $S_\infty(\mathcal{K})$ se descompone totalmente en F . Por la Proposición 12.3.4, $F \subseteq K(\Lambda_N)\mathbb{F}_{q^m}$ para algunos $N \in R_T$ y $m \in \mathbb{N}$. En el caso de que $F \subseteq K(\Lambda_N)$, sea Z el grupo de caracteres de Dirichlet asociado a F . Puesto que F/\mathcal{K} es no ramificada, se sigue que $X \subseteq Z \subseteq Y$ debido a la Proposición 12.3.3 y por tanto $F \subseteq J$. Puesto que $J^{(2)} = J^{\mathfrak{D}}$, obtenemos que $F \subseteq J^{(2)}$.



Para el caso general $K \subseteq F \subseteq K(\Lambda_N)\mathbb{F}_{q^m}$, sea \mathfrak{I} el grupo de inercia de $S_\infty(\mathcal{K})$ en $K(\Lambda_N)/\mathcal{K}$ y sea $B := K(\Lambda_N)^{\mathfrak{I}}$. Entonces $S_\infty(B)$ es totalmente inerte en B_m debido a que tiene grado 1 y $S_\infty(B)$ es totalmente ramificado en $K(\Lambda_N)/B$. Como $S_\infty(\mathcal{K})$ se descompone totalmente en B , B es el campo de descomposición de $S_\infty(\mathcal{K})$ en $K(\Lambda_N)_m/\mathcal{K}$ por lo que $F \subseteq B \subseteq K(\Lambda_N)$.

De la primera parte, obtenemos que $F \subseteq J^{(2)}$. De esta forma se ha probado el siguiente

Teorema 12.3.6. *Supongamos que $\mathcal{K} \subseteq K(\Lambda_N)$ para algún polinomio N . Sean X el grupo de caracteres de Dirichlet asociado a \mathcal{K} , $Y = \prod_{P|N} X_P$, $Y_1 = \{\chi \in Y \mid \chi(a) = 1 \text{ para toda } a \in \mathbb{F}_q^*\}$ y $J^{(1)}$ el campo asociado a Y_1 . Entonces el campo de géneros de \mathcal{K} es $\mathcal{K}\mathfrak{ge} = \mathcal{K}J^{(1)}$. \square*

12.3.1. Campos de funciones congruentes generales

Primero probaremos el siguiente resultado.

Lema 12.3.7. *Si \mathcal{K}/K es una extensión abeliana y de grado el grado de cualquier divisor primo en $S_\infty(\mathcal{K})$, digamos t , entonces el campo de constantes de \mathcal{K}_{ge} es \mathbb{F}_{q^t} .*

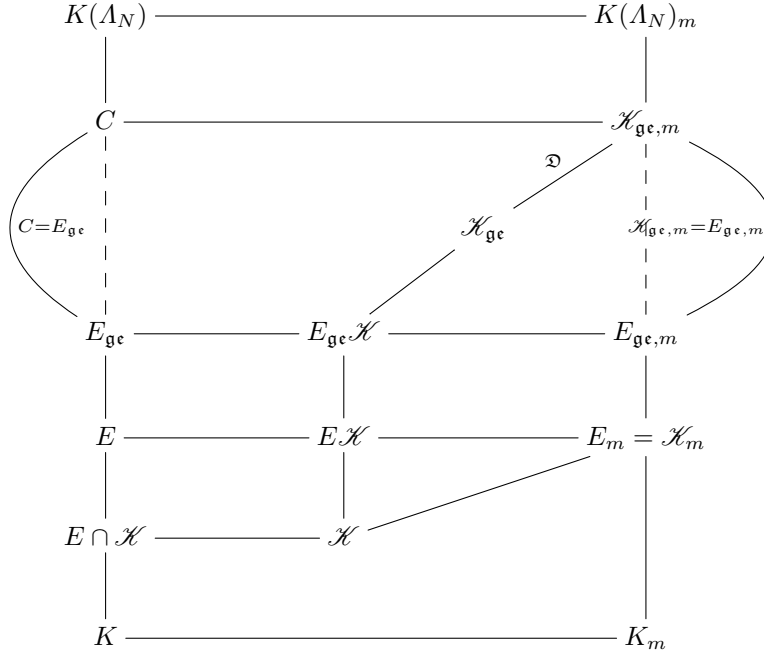
Demostración. Consideremos la extensión de constantes $\mathcal{K}_r := \mathcal{K}\mathbb{F}_{q^r}$ de \mathcal{K} . Entonces el número de primos en \mathcal{K}_r sobre cualquier primo en $S_\infty(\mathcal{K})$ es $h = \text{mcd}(d_{\mathcal{K}}(S_\infty(\mathcal{K})), r) = \text{mcd}(t, r)$ ([70, Theorem 6.2.1(2)]). Por lo tanto $S_\infty(\mathcal{K})$ se descompone completamente en $\mathcal{K}_r/\mathcal{K}$ si y sólo si $h = r$ y esto es equivalente a $r \mid d_{\mathcal{K}}(S_\infty(\mathcal{K})) = t$. Se sigue que la máxima extensión de constantes de \mathcal{K} en donde $S_\infty(\mathcal{K})$ se descompone totalmente es $\mathcal{K}_t = \mathcal{K}\mathbb{F}_{q^t}$. Luego el campo de constantes de \mathcal{K}_{ge} es \mathbb{F}_{q^t} . \square

Ahora consideramos cualquier extensión abeliana geométrica \mathcal{K}/\mathbb{F}_q de K tal que \mathfrak{p}_∞ es moderadamente ramificado. Entonces tenemos que $\mathcal{K} \subseteq K(\Lambda_N)\mathbb{F}_{q^m} = K(\Lambda_N)_m$ para algunos $N \in R_T$ y $m \in \mathbb{N}$. Puesto que $K(\Lambda_N)/K$ es una extensión geométrica y K_m/K es una extensión de constantes, tenemos $K(\Lambda_N) \cap K_m = K$. Puesto que \mathfrak{p}_∞ es moderadamente ramificado en $\mathcal{K}_{\text{ge}}/K$, sin pérdida de generalidad, podemos suponer que $\mathcal{K}_{\text{ge}} \subseteq K(\Lambda_N)_m$.

Definamos $E := \mathcal{K}_m \cap K(\Lambda_N) \subseteq \mathcal{K}_m$. Entonces $E_m \subseteq \mathcal{K}_m$. Por otro lado $[\mathcal{K}_m : K] = [\mathcal{K}_m : K_m][K_m : K] = [E : K][K_m : K] = [E_m : K_m][K_m : K] = [E_m : K]$. Por lo tanto $E_m = \mathcal{K}_m$. También tenemos $[E : K] = [\mathcal{K} : K]$ puesto que $m[\mathcal{K} : K] = [\mathcal{K}_m : K] = [E_m : K] = m[E : K]$. En otras palabras, E juega un papel similar al de \mathcal{K} pero está contenido en una extensión ciclotómica.

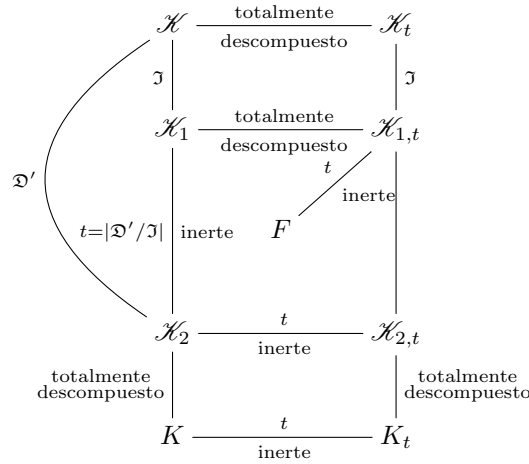
Puesto que $E = \mathcal{K}_m \cap K(\Lambda_N)$, se sigue que $E \cap \mathcal{K} = E_{\text{ge}} \cap \mathcal{K} = K(\Lambda_N) \cap \mathcal{K}$. Ya que $\mathcal{K}_m/\mathcal{K}$ y E_{ge}/E son no ramificadas, obtenemos que $E_{\text{ge}}\mathcal{K}/\mathcal{K}$ es no ramificada. También, puesto que $S_\infty(E)$ se descompone totalmente en E_{ge} , $S_\infty(E\mathcal{K})$ se descompone totalmente en $E_{\text{ge}}\mathcal{K}$. Ahora bien, $S_\infty(E \cap \mathcal{K})$ tiene grado de inercia uno en $E/(E \cap \mathcal{K})$, por lo que $S_\infty(\mathcal{K})$ tiene grado de inercia uno en $E\mathcal{K}/\mathcal{K}$. Por tanto $E_{\text{ge}}\mathcal{K} \subseteq \mathcal{K}_{\text{ge}}$. Finalmente, si $C := \mathcal{K}_{\text{ge},m} \cap K(\Lambda_N)$, por un lado $E_{\text{ge}} \subseteq C$ y por otro lado C/E es no ramificado puesto que $\mathcal{K}_{\text{ge}}/E\mathcal{K}$, $\mathcal{K}_{\text{ge},m}/\mathcal{K}_{\text{ge}}$ y $E\mathcal{K}/E$ son no ramificados; también $S_\infty(E)$ se descompone totalmente en C/E puesto que $C \subseteq K(\Lambda_N)$. Se sigue que $C \subseteq E_{\text{ge}}$. Así, $C = E_{\text{ge}}$.

Por tanto, como $K(\Lambda_N)_m = K(\Lambda_N)K_m$ y $K(\Lambda_N) \cap K_m = K$, por la correspondencia de Galois, tenemos $\mathcal{K}_{\text{ge},m} = E_{\text{ge},m}$.



También se tiene que $(E_{\mathfrak{g}\mathfrak{e}}\mathcal{K})_m = E_{\mathfrak{g}\mathfrak{e}}\mathcal{K}_m = E_{\mathfrak{g}\mathfrak{e},m} = \mathcal{K}_{\mathfrak{g}\mathfrak{e},m}$. Luego $\mathcal{K}_{\mathfrak{g}\mathfrak{e},m}/E_{\mathfrak{g}\mathfrak{e}}\mathcal{K}$ es una extensión de constantes y $E_{\mathfrak{g}\mathfrak{e}}\mathcal{K} \subseteq \mathcal{K}_{\mathfrak{g}\mathfrak{e}} \subseteq \mathcal{K}_{\mathfrak{g}\mathfrak{e},m}$. Entonces $\mathcal{K}_{\mathfrak{g}\mathfrak{e}}/E_{\mathfrak{g}\mathfrak{e}}\mathcal{K}$ es una extensión de constantes. Por el Lema 12.3.7, el campo de constantes de $\mathcal{K}_{\mathfrak{g}\mathfrak{e}}$ es \mathbb{F}_{q^t} , así que $\mathcal{K}_{\mathfrak{g}\mathfrak{e}} = (E_{\mathfrak{g}\mathfrak{e}}\mathcal{K})_t$. Si probamos que $\mathbb{F}_{q^t} \subseteq E_{\mathfrak{g}\mathfrak{e}}\mathcal{K}$, se seguirá que $\mathcal{K}_{\mathfrak{g}\mathfrak{e}} = E_{\mathfrak{g}\mathfrak{e}}\mathcal{K}$.

Sea \mathfrak{I} el grupo de inercia de cualquier elemento de $S_\infty(\mathcal{K})$ en la extensión \mathcal{K}/K , $|\mathfrak{I}| = e(S_\infty(\mathcal{K}) \mid \mathfrak{p}_\infty) = e$, y sea \mathfrak{D}' el grupo de descomposición de $S_\infty(\mathcal{K})$ en \mathcal{K}/K . Tenemos que $|\mathfrak{D}'| = et$ puesto que $\mathfrak{D}'/\mathfrak{I} \cong \text{Gal}(\mathcal{K}(S_\infty(\mathcal{K}))/K(\mathfrak{p}_\infty)) \cong C_t$. En el siguiente diagrama, el tipo de descomposición es con referencia a los divisores primos infinitos.



Aquí $\mathcal{H}_1 := \mathcal{H}^{\mathfrak{J}}$, $\mathcal{H}_2 := \mathcal{H}^{\mathfrak{D}'}$ y F es el campo fijo del grupo de descomposición de \mathfrak{p}_{∞} en $\mathcal{H}_{1,t}/K$. Se sigue que \mathfrak{p}_{∞} es totalmente descompuesto en F/K . Por lo tanto $F \subseteq K(A_N)$. El grado de inercia de cualquier elemento de $S_{\infty}(\mathcal{H}_2)$ en la extensión $\mathcal{H}_1/\mathcal{H}_2$ es t . Por lo tanto $F \cap \mathcal{H}_1 = \mathcal{H}_2$ y $F\mathcal{H}_1/\mathcal{H}_2$ es una extensión de grado t^2 con grupo de Galois $C_t \times C_t$. En particular obtenemos $F\mathcal{H}_1 = \mathcal{H}_{1,t}$.

Puesto que $F \subseteq \mathcal{H}_t$ y $\mathcal{H} \subseteq K(\Lambda_N)_m$, tenemos $F \subseteq \mathcal{H}_t \subseteq (K(\Lambda_N)_m)_t = K(\Lambda_N)_m$. Ya que $E = \mathcal{H}_m \cap K(\Lambda_N)$ se sigue que $F \subseteq E$. Obtenemos $K_t \mathcal{H}_1 = \mathcal{H}_{1,t} = F \mathcal{H}_1 \subseteq F \mathcal{H} \subseteq E \mathcal{H}$. Por lo tanto, el campo de constantes de $E \mathcal{H}$ contiene a K_t . De aquí $\mathcal{H}_{\mathbf{gc}} = E_{\mathbf{gc}} \mathcal{H}$.

Recordemos que $\mathcal{K}_{\mathfrak{ge},m} = E_{\mathfrak{ge},m}$. Por lo tanto $\mathcal{K}_{\mathfrak{ge}} = E_{\mathfrak{ge},m}^{\mathfrak{D}}$ donde \mathfrak{D} es el grupo de descomposición de los divisores primos en $S_{\infty}(\mathcal{K})$ en $E_{\mathfrak{ge},m}/\mathcal{K}$. Observemos que $|\mathfrak{D}| = [\mathcal{K}_{\mathfrak{ge},m} : \mathcal{K}_{\mathfrak{ge}}] = \frac{m}{t}$ donde t es el grado de cualquier primo en $S_{\infty}(\mathcal{K})$.

Se ha probado

Teorema 12.3.8. *Sea \mathcal{K}/\mathbb{F}_q una extensión abeliana finita geométrica de K donde \mathfrak{p}_∞ es moderadamente ramificado. Sea $N \in R_T$ y $m \in \mathbb{N}$ es tal que $\mathcal{K} \subseteq K(N_N)\mathbb{F}_{q^m}$. Sea $E_{\mathfrak{g}\mathfrak{c}}$ el campo de géneros de $E := K(N_N) \cap \mathcal{K}\mathbb{F}_{q^m}$ y sea $E_{\mathfrak{g}\mathfrak{c},m} = E_{\mathfrak{g}\mathfrak{c}}\mathbb{F}_{q^m}$. Sea \mathfrak{D} el grupo de descomposición de los divisores primos en $S_\infty(\mathcal{K})$ en $E_{\mathfrak{g}\mathfrak{c},m}$. Entonces, el campo de géneros de \mathcal{K} es $\mathcal{K}_{\mathfrak{g}\mathfrak{c}} = E_{\mathfrak{g}\mathfrak{c},m}^{\mathfrak{D}} = E_{\mathfrak{g}\mathfrak{c}}\mathcal{K}$.*

Observación 12.3.9. Sea $\langle \sigma \rangle = \text{Gal}(K(\Lambda_N)_m/K(\Lambda_N)) \cong \text{Gal}(K_m/K)$. Entonces, con las notaciones anteriores, se tiene $\mathfrak{D} \cong \langle \sigma^t \rangle$ y

$$[\mathcal{K}_{\text{gc}} : \mathcal{K}] = \frac{[E_{\text{gc},m} : \mathcal{K}]}{|\mathfrak{D}|} = \frac{[E_{\text{gc},m} : \mathcal{K}_m][\mathcal{K}_m : \mathcal{K}]}{m/t} = [E_{\text{gc}} : E]t,$$

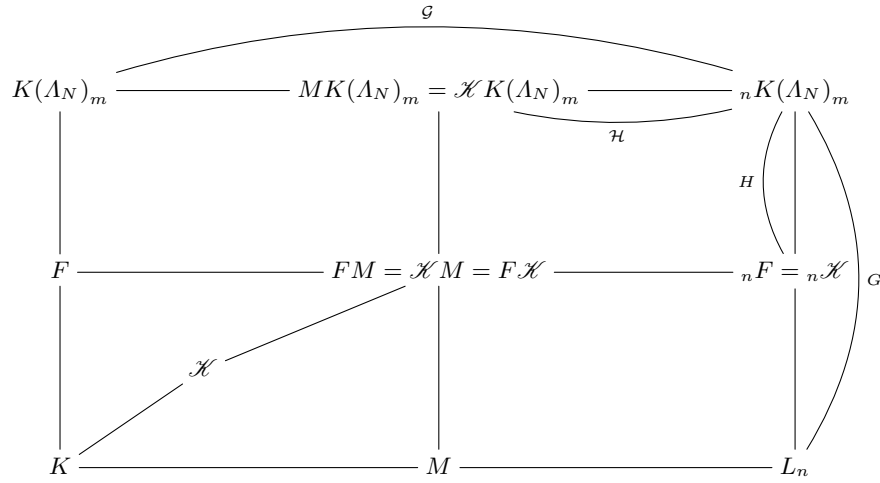
donde t es el grado de cualquier primo en $S_\infty(\mathcal{K})$.

Finalmente consideremos cualquier extensión abeliana finita \mathcal{K} de K . Por el Teorema de Kronecker–Weber se tiene $\mathcal{K} \subseteq K(\Lambda_N)\mathbb{F}_{q^m}L_n = {}_nK(\Lambda_N)_m$ para algunas $N \in R_T$ y $n, m \in \mathbb{N}$.

Sean $\mathcal{G} := \text{Gal}({}_nK(\Lambda_N)_m/K(\Lambda_N)_m)$, $\mathcal{H} := \text{Gal}({}_nK(\Lambda_N)_m/\mathcal{K}K(\Lambda_N)_m)$, $M := \mathcal{K}K(\Lambda_N)_m \cap L_n = L_n^{\mathcal{H}_1}$ donde $\mathcal{H}_1 := \mathcal{H}|_{L_n}$.

Sea $G := \text{Gal}({}_nK(\Lambda_N)_m/L_n)$, $H := \text{Gal}({}_nK(\Lambda_N)_m/{}_n\mathcal{K})$, $F := {}_n\mathcal{K} \cap K(\Lambda_N)_m = K(\Lambda_N)_m^{H_1}$ donde $H_1 := H|_{K(\Lambda_N)_m}$.

Tenemos que $F = {}_n\mathcal{K} \cap K(\Lambda_N)_m \subseteq {}_n\mathcal{K}$. Por tanto, por un lado ${}_nF \subseteq {}_n\mathcal{K}$, y por otro lado $[{}_nK(\Lambda_N)_m : {}_nF] = [K(\Lambda_N)_m : F] = |H_1| = |H| = [{}_nK(\Lambda_N)_m : {}_n\mathcal{K}]$. Se sigue que ${}_nF = {}_n\mathcal{K}$. Similarmente se obtiene $MK(\Lambda_N)_m = \mathcal{K}K(\Lambda_N)_m$.



Sea $A \subseteq \mathcal{G} \times G$ tal que $\mathcal{K} = {}_nK(\Lambda_M)K(\Lambda_M)_m^A$. Primero probaremos que $FM = \mathcal{K}M = F\mathcal{K}$. Se tiene que $F = {}_nK(\Lambda_N)_m^{\mathcal{G} \times H}$ y $M = {}_nK(\Lambda_N)_m^{\mathcal{H} \times G}$. Entonces si denotamos $R = {}_nK(\Lambda_N)_m$, tenemos

$$\begin{aligned} R^{A \cap (\mathcal{G} \times 1)} &= R^A R^{\mathcal{G} \times 1} = \mathcal{K}K(\Lambda_N)_m = MK(\Lambda_N)_m \\ &= R^{\mathcal{H} \times G} R^{\mathcal{G} \times 1} = R^{(\mathcal{H} \times G) \cap (\mathcal{G} \times 1)} = R^{\mathcal{H} \times 1}, \end{aligned}$$

así que $A \cap (\mathcal{G} \times 1) = \mathcal{H} \times 1$. Similarmente $A \cap (1 \times G) = 1 \times H$. Por lo tanto

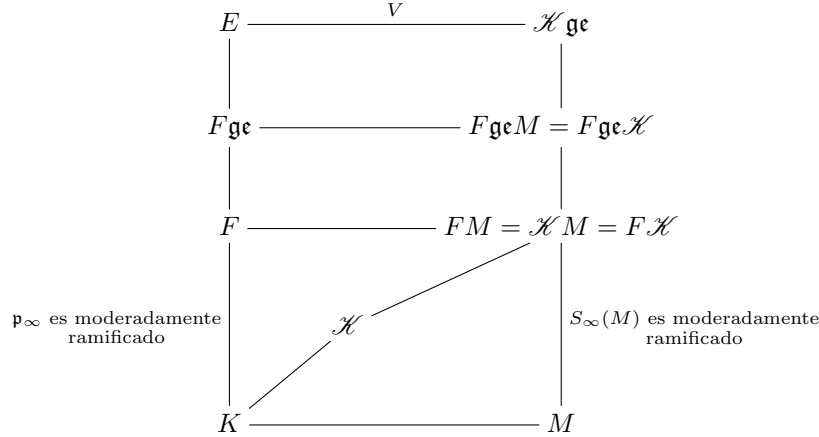
$$\begin{aligned} FM &= R^{\mathcal{G} \times H} R^{\mathcal{H} \times G} = R^{(\mathcal{G} \times H) \cap (\mathcal{H} \times G)} = R^{\mathcal{H} \times H}, \\ \mathcal{K}M &= R^A R^{\mathcal{H} \times G} = R^{A \cap (\mathcal{H} \times G)}, \\ F\mathcal{K} &= R^{\mathcal{G} \times H} R^A = R^{(\mathcal{G} \times H) \cap A}. \end{aligned}$$

Puesto que es fácil ver que $(\mathcal{G} \times H) \cap A = A \cap (\mathcal{H} \times G) = \mathcal{H} \times H$, se sigue que $FM = \mathcal{K}M = F\mathcal{K}$.

Dado que $F\mathfrak{ge}/F$ es no ramificado y $S_\infty(F)$ se descompone totalmente, obtenemos que ${}_n\mathcal{K}F\mathfrak{ge}/{}_n\mathcal{K}$ es no ramificada y $S_\infty({}_nF)$ se descompone totalmente. Ahora, en ${}_n\mathcal{K}/\mathcal{K}$ el único posible primo ramificado es $S_\infty(\mathcal{K})$ y si esto es así, es salvajemente ramificado. Se sigue que en ${}_n\mathcal{K}F\mathfrak{ge}/\mathcal{K}$ el único posible primo ramificado es $S_\infty(\mathcal{K})$ y en caso de ser así, es salvajemente ramificado. En particular en $F\mathfrak{ge}\mathcal{K}/\mathcal{K}$ el único posible primo ramificado es $S_\infty(\mathcal{K})$ y si se ramifica, es salvajemente ramificado.

Nuevamente, dado que la extensión $F\mathfrak{ge}/F$ es no ramificada y $S_\infty(F)$ se descompone totalmente, $F\mathfrak{ge}\mathcal{K}/F\mathcal{K}$ es no ramificada y $S_\infty(F\mathcal{K})$ se descompone totalmente. En la extensión $F/(\mathcal{K} \cap F)$, $S_\infty(\mathcal{K} \cap F)$ es moderadamente ramificada, de aquí que $S_\infty(\mathcal{K})$ es moderadamente ramificado en $F\mathcal{K}/\mathcal{K}$. Por lo tanto $S_\infty(\mathcal{K})$ se descompone totalmente en $F\mathcal{K}/\mathcal{K}$. En resumen, tenemos que $F\mathfrak{ge}\mathcal{K} \subseteq \mathcal{K}\mathfrak{ge}$.

Puesto que $FM = F\mathcal{K}$, $F\mathfrak{ge}M = F\mathfrak{ge}\mathcal{K} \subseteq \mathcal{K}\mathfrak{ge}$. Sea V el primer grupo de ramificación de \mathfrak{p}_∞ en $\mathcal{K}\mathfrak{ge}/K$. Sea $E := \mathcal{K}\mathfrak{ge}^V$. Entonces \mathfrak{p}_∞ es moderadamente ramificado en E/K y por lo tanto $E \subseteq K(\Lambda_N)_m$. Obtenemos que $S_\infty(M)$ es moderadamente ramificado en $\mathcal{K}\mathfrak{ge}/M$ y puesto que $\mathcal{K}\mathfrak{ge}/\mathcal{K}$ es no ramificado, se sigue que $\mathcal{K}\mathfrak{ge}/FM$ es no ramificado. Finalmente \mathfrak{p}_∞ es moderadamente ramificado en F/K así que $S_\infty(M)$ es moderadamente ramificado en FM/M . Puesto que \mathfrak{p}_∞ es total y salvajemente ramificado en M/K , $M \cap E = K$.



Ahora $[\mathcal{K}\mathfrak{ge} : K] = [E : K][V] = [E : K][M : K] = [EM : K]$. Se sigue que $\mathcal{K}\mathfrak{ge} = EM$. Tenemos que $F\mathfrak{ge} \subseteq E$ puesto que $F\mathfrak{ge} = F\mathfrak{ge}\mathcal{K} \cap E \subseteq E$. La extensión es no ramificada así que $\mathcal{K}\mathfrak{ge}/F\mathcal{K}$ es no ramificada y el único posible primo ramificado en $F\mathcal{K} = FM/F$ es $S_\infty(F)$ y en caso de ser así, es salvajemente ramificado. $S_\infty(F)$ es no ramificado en E/F ya que de otra forma sería moderadamente ramificado, y E/F es no ramificado en cualquier otro primo puesto que $\mathcal{K}\mathfrak{ge}/F$ es ramificado en a lo más en $S_\infty(F)$. Se sigue que $E \subseteq F\mathfrak{ge}$ y por lo tanto $E = F\mathfrak{ge}$. Entonces $\mathcal{K}\mathfrak{ge} = EM = F\mathfrak{ge}M = F\mathfrak{ge}\mathcal{K}$.

Se ha probado:

Teorema 12.3.10. *Sea \mathcal{K}/K cualquier extensión finita abeliana tal que $\mathcal{K} \subseteq {}_n K(\Lambda_N)_m$. Sea $F = {}_n \mathcal{K} \cap K(\Lambda_N)_m$ y $M = \mathcal{K} K(\Lambda_N)_m \cap L_n$. Entonces el campo de géneros de \mathcal{K} es $\mathcal{K} \mathbf{ge} = F \mathbf{ge} \mathcal{K} = F \mathbf{ge} M$. \square*

Nuestro resultado principal en esta sección es la combinación de los Teoremas 12.3.8 y 12.3.10.

Teorema 12.3.11. *Sea \mathcal{K}/K una extensión abeliana finita que satisface $\mathcal{K} \subseteq K(\Lambda_N) \mathbb{F}_{q^m} L_n$. Sea $F = \mathcal{K} L_n \cap K(\Lambda_N) \mathbb{F}_{q^m}$ y $E = K(\Lambda_N) \cap F \mathbb{F}_{q^m}$. Entonces el campo de géneros de \mathcal{K} es $\mathcal{K} \mathbf{ge} = E \mathbf{ge} F \mathcal{K}$ donde $E \mathbf{ge}$ es el campo de géneros de E . \square*

12.3.2. Aplicaciones

En esta sección veremos como los resultados anteriores pueden ser aplicados a algunas extensiones abelianas generales: las extensiones de Kummer, de Artin–Schreier y las p -extensiones cíclicas (Witt).

Extensiones de Kummer

Aquí supondremos que $q \geq 3$. Primeramente queremos saber cuando un campo $K(\sqrt[l]{P})$, donde $l \mid q-1$ y $P \in R_T^+$, está contenido en $K(\Lambda_P)$. Por la Proposición 9.5.13 se tiene que $K(\sqrt[l]{(-1)^d P}) \subseteq K(\Lambda_P)$. El grupo de Galois $\text{Gal}(K(\Lambda_P)/K) \cong (R_T/(P))^* \cong \mathbb{F}_{q^d}^*$ es un grupo cíclico de orden $q^d - 1$, donde d es el grado de P . Por lo tanto existe una única extensión de la forma $K(\sqrt[l]{\alpha P})$, $\alpha \in \mathbb{F}_q^*$, contenido en $K(\Lambda_P)$. Notemos que si $\alpha \notin (\mathbb{F}_q^*)^l$, $K(\sqrt[l]{P}) \neq K(\sqrt[l]{\alpha P})$ puesto que de otra forma $\sqrt[l]{\alpha} \in K$ y así $\alpha \in (\mathbb{F}_q^*)^l$.

Usaremos que para cualquier $\alpha \in \mathbb{F}_q^*$, $1 \leq e \leq l-1$, $K(\sqrt[l]{\alpha P^e}) = K(\sqrt[l]{\alpha^f P})$ donde $fe \equiv 1 \pmod{l}$. Puesto que tenemos l clases mód $(\mathbb{F}_q^*)^l$ en \mathbb{F}_q^* , los l campos distintos $K(\sqrt[l]{\alpha P})$, $\alpha \in \mathbb{F}_q^*$ están dados por las clases mód $(\mathbb{F}_q^*)^l$. Por lo tanto $K(\sqrt[l]{\alpha^f P}) \subseteq K(\Lambda_P)$ si y sólo si $\alpha^f \equiv (-1)^d \pmod{(\mathbb{F}_q^*)^l}$.

En esta subsección usaremos las notaciones de la Sección 12.3.1. En esta situación tenemos $m = l$. Sea $\mathcal{K} := K(\sqrt[l]{\gamma D})$ donde $D \in R_T$ es un polinomio mónico sin factores que sean l potencias, $\gamma \in \mathbb{F}_q^*$ y $D = P_1^{e_1} \cdots P_r^{e_r}$ donde $P_i \in R_T^+$, $1 \leq e_i \leq l-1$, $1 \leq i \leq r$. Más aún arreglamos el producto de tal forma que $l \mid \text{gr } P_i$ para $1 \leq i \leq s$ y $l \nmid \text{gr } P_j$ para $s+1 \leq j \leq r$, $0 \leq s \leq r$. En general, siempre se tiene que $E = K(\sqrt[l]{(-1)^{\text{gr } D} D})$, y $\mathbb{F}_q^* \subseteq (\mathbb{F}_{q^l}^*)^l$.

Primero,

Proposición 12.3.12. *El comportamiento de \mathfrak{p}_∞ en \mathcal{K}/K es el siguiente:*

- (i) Si $l \nmid \text{gr } D$, \mathfrak{p}_∞ es ramificado.
- (ii) Si $l \mid \text{gr } D$ y $\gamma \in (\mathbb{F}_q^*)^l$, \mathfrak{p}_∞ se descompone.

(III) Si $l \mid \text{gr } D$ y $\gamma \notin (\mathbb{F}_q^*)^l$, \mathfrak{p}_∞ es inerte.

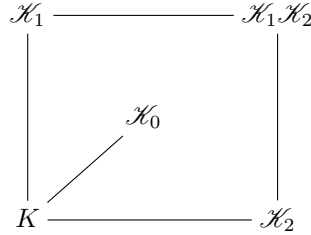
Demostración. Sea \mathfrak{P}_∞ un divisor primo en \mathcal{K} sobre \mathfrak{p}_∞ . Sean $\beta := \sqrt[l]{\gamma D}$, $d := \text{gr } D$ y $e := e(\mathfrak{P}_\infty | \mathfrak{p}_\infty)$. Si $l \nmid \text{gr } D$, entonces

$$lv_{\mathfrak{P}_\infty}(\beta) = v_{\mathfrak{P}_\infty}(\beta^l) = v_{\mathfrak{P}_\infty}(\gamma D) = v_{\mathfrak{P}_\infty}(D) = ev_{\mathfrak{p}_\infty}(D) = -ed,$$

por lo que $l \mid -ed$ y puesto que $l \nmid d$, se sigue que $l \mid e$ y por tanto \mathfrak{p}_∞ es ramificado en \mathcal{K}/K .

Ahora consideremos el caso en que $l \mid d$. Sea $d = ld_1$. Se tiene que $\mathcal{K}_0 := K(\sqrt[l]{(-1)^{\text{gr } D} D}) = K((-1)^{d_1} \sqrt[l]{D}) = K(\sqrt[l]{D}) \subseteq K(\Lambda_D)$. Veamos que \mathfrak{p}_∞ se descompone en \mathcal{K}_0/K . Sea $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ con $P_1, P_2, \dots, P_r \in R_T^+$ distintos. Si $r = 1$, puesto que $[K(\Lambda_{P_1^{\alpha_1}}) : K(\Lambda_{P_1})] = q^{(\alpha_1-1)\text{gr } P_1}$ es primo relativo a l , se tiene que $\mathcal{K}_0 \subseteq K(\Lambda_{P_1})$. Sea $s = \text{gr } P_1$, entonces $\frac{q^s-1}{q-1} = (q^{s-1} + \cdots + q + 1) \equiv d \pmod{q-1}$ por lo que $l \mid \frac{q^s-1}{q-1}$. Esto implica en particular se tiene que el único grupo H del grupo cíclico $\text{Gal}(K(\Lambda_{P_1})/K)$ de orden $\frac{q^s-1}{q-1}$, el cual contiene a \mathbb{F}_q^* , satisface que $\mathcal{K} \subseteq K(\Lambda_{P_1})^H$. En particular \mathfrak{p}_∞ se descompone en \mathcal{K}/K .

Para el caso $r \geq 2$ se tiene que \mathfrak{p}_∞ es ramificado tanto en el campo $\mathcal{K}_1 := K(\sqrt[l]{P_1^{\alpha_1} \cdots P_{r-1}^{\alpha_{r-1}}})$ como en el campo $\mathcal{K}_2 := K(\sqrt[l]{P_r^{\alpha_r}})$ pues como $l \mid d = \sum_{i=1}^r \alpha_i \text{gr } P_i = \sum_{i=1}^{r-1} \alpha_i \text{gr } P_i + \alpha_r \text{gr } P_r$ y $l \nmid \alpha_r \text{gr } P_r$, entonces $l \nmid \sum_{i=1}^{r-1} \alpha_i \text{gr } P_i = \text{gr}(P_1^{\alpha_1} \cdots P_{r-1}^{\alpha_{r-1}})$. Por el Lema de Abhyankar (o por ser moderadamente ramificado), el grado de ramificación de \mathfrak{p}_∞ en $\mathcal{K}_1 \mathcal{K}_2/K$, existe un único campo \mathcal{K}_0 de grado l sobre K y contenido en $\mathcal{K}_1 \mathcal{K}_2$ donde \mathfrak{p}_∞ es no ramificado, a saber, el campo correspondiente al grupo de inercia de \mathfrak{p}_∞ en $\mathcal{K}_1 \mathcal{K}_2/K$.



Los campos de grado l sobre K contenidos en $\mathcal{K}_1 \mathcal{K}_2$ son precisamente $K(\sqrt[l]{P_1^{\alpha_1} \cdots P_{r-1}^{\alpha_{r-1}} P_r^{j\alpha_r}})$, $0 \leq j \leq l-1$ y \mathcal{K}_1 . Se tiene que $l \nmid d = \sum_{i=1}^{r-1} \alpha_i \text{gr } P_i + j\alpha_r \text{gr } P_r = d + (j-1)\alpha_r \text{gr } P_r$ para $j \neq 1$ por lo que $\mathcal{K}_0 = \mathcal{K}$ y \mathfrak{p}_∞ se descompone en \mathcal{K}/K .

Ahora sea $\mu \in \mathbb{F}_q \setminus (\mathbb{F}_q^*)^l$. Entonces $\mathbb{F}_{q^l} = \mathbb{F}_q(\sqrt[l]{\mu})$ y $\sqrt[l]{\mu} \notin \mathbb{F}_q^*$. Por la discusión anterior tenemos que \mathfrak{p}_∞ es inerte en $\mathbb{F}_{q^l}(T) = K(\sqrt[l]{\mu})$ y descompuesto en $K(\sqrt[l]{D})$. Los campos de grado l sobre K contenidos en $K(\sqrt[l]{\mu}, \sqrt[l]{D})$ son $K(\sqrt[l]{\mu})$ y $K(\sqrt[l]{\mu^j D})$ para $j = 0, 1, \dots, l-1$. Como el grupo de descomposición de \mathfrak{p}_∞ en $K(\sqrt[l]{\mu}, \sqrt[l]{D})/K$ es de orden l , se sigue \mathfrak{p}_∞ es inerte en todo

campo $K(\sqrt[l]{\mu^j D})$, $0 \leq j \leq l-1$. Si $\gamma \in (\mathbb{F}_q^*)^l$ se tiene $\mathcal{K} = K(\sqrt[l]{\gamma D})$ y \mathfrak{p}_∞ se descompone en \mathcal{K}/K . Si $\gamma \notin (\mathbb{F}_q^*)^l$ entonces $\mathcal{K} = K(\sqrt[l]{\mu^j D})$ para algún $j = 1, \dots, l-1$ y \mathfrak{p}_∞ es inerte en \mathcal{K}/K . \square

Ahora por la Observación 12.3.9, tenemos que $[\mathcal{K}^{\mathfrak{ge}} : \mathcal{K}] = [E^{\mathfrak{ge}} : E]t$ donde

$$t = \text{gr } S_\infty(\mathcal{K}) = \begin{cases} 1 & \text{si } \mathfrak{p}_\infty \text{ no es inerte en } \mathcal{K}/K \\ l & \text{si } \mathfrak{p}_\infty \text{ es inerte en } \mathcal{K}/K. \end{cases}$$

Cuando $\mathcal{K} = E$, esto es, cuando $\mathcal{K} \subseteq K(\Lambda_D)$, si χ es el caracter de orden l asociado a \mathcal{K} , $\chi = \chi_{P_1} \cdots \chi_{P_r}$, consideramos $Y = \langle \chi_{P_i} \mid 1 \leq i \leq r \rangle$. El campo asociado a Y es $F = K(\sqrt[l]{(-1)^{\text{gr } P_1} P_1}, \dots, \sqrt[l]{(-1)^{\text{gr } P_r} P_r})$ y $\mathcal{K}^{\mathfrak{ge}} = F$ si $l \nmid \text{gr } D$ o si $l \mid \text{gr } P_i$ para toda i (esto es, $s = r$). Esto es así puesto que en el primer caso \mathfrak{p}_∞ es ya ramificado en \mathcal{K} y en segundo \mathfrak{p}_∞ es no ramificado en F/K (Proposición 12.3.12).

Cuando $l \mid \text{gr } D$ y $l \nmid \text{gr } P_r$, \mathfrak{p}_∞ se ramifica en F/K y es no ramificado en E/K . En este caso $[F : E^{\mathfrak{ge}}] = l$. Sea $a_{s+1}, \dots, a_{r-1} \in \mathbb{Z}$ tales que $l \mid \text{gr}(P_i P_r^{a_i})$, esto es, $\text{gr } P_i + a_i \text{gr } P_r \equiv 0 \pmod{l}$, $s+1 \leq i \leq r-1$. Sea

$$F_1 := K(\sqrt[l]{P_1}, \dots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1} P_r^{a_{s+1}}}, \dots, \sqrt[l]{P_{r-1} P_r^{a_{r-1}}}) \subseteq K(\Lambda_{P_1 P_2 \dots P_r}).$$

Entonces $S_\infty(E)$ se descompone en F_1/E , $\mathcal{K} \subseteq F_1 \subseteq E^{\mathfrak{ge}}$ y $[F : F_1] = l$. se sigue que $E^{\mathfrak{ge}} = F_1$.

En el caso general, del Teorema 12.3.10 obtenemos $\mathcal{K}^{\mathfrak{ge}} = E^{\mathfrak{ge}} \mathcal{K}$. Por lo tanto

Teorema 12.3.13. *Sea $D = P_1^{e_1} \cdots P_r^{e_r} \in R_T$ un polinomio mónico que no tiene l potencias, donde $P_i \in R_T^+$, $1 \leq e_i \leq l-1$, $1 \leq i \leq r$. Sea $0 \leq s \leq r$ tal que $l \mid \text{gr } P_i$ para $1 \leq i \leq s$ y $l \nmid \text{gr } P_j$ para $s+1 \leq j \leq r$. Sea $\mathcal{K} := K(\sqrt[l]{\gamma D})$ donde $\gamma \in \mathbb{F}_q^*$. Entonces $\mathcal{K}^{\mathfrak{ge}}$ está dado por:*

- (i) $K(\sqrt[l]{\gamma D}, \sqrt[l]{(-1)^{\text{gr } P_1} P_1}, \dots, \sqrt[l]{(-1)^{\text{gr } P_r} P_r})$ si $l \nmid \text{gr } D$ o si $l \mid \text{gr } P_i$ para toda $1 \leq i \leq r$,
- (ii) $K(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \dots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1} P_r^{a_{s+1}}}, \dots, \sqrt[l]{P_{r-1} P_r^{a_{r-1}}})$, donde el exponente a_j satisface $\text{gr } P_j + a_j \text{gr } P_r \equiv 0 \pmod{l}$, $s+1 \leq j \leq r-1$, si $l \mid \text{gr } D$ y $l \nmid \text{gr } P_r$.

Extensiones de Artin–Schreier

Consideremos $\mathcal{K} := K(y)$ donde $y^p - y = \alpha \in K$. La ecuación puede ser normalizada como sigue:

$$y^p - y = \alpha = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}} + f(T), \quad (12.23)$$

donde $P_i \in R_T^+$, $Q_i \in R_T$, $\text{mcd}(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\text{gr } Q_i < \text{gr } P_i^{e_i}$, $1 \leq i \leq r$, $f(T) \in R_T$, con $p \nmid \text{gr } f$ cuando $f(T) \notin \mathbb{F}_q$.

Tenemos que los primos finitos ramificados en \mathcal{K}/K son precisamente P_1, \dots, P_r . Con respecto a \mathfrak{p}_∞ tenemos la Proposición 12.2.5.

Estudiamos dos casos.

Caso 1: Suponemos en este caso que \mathfrak{p}_∞ es no ramificado, así que $f(T) \in \mathbb{F}_q$. Tenemos $\text{Gal}(\mathcal{K}_p/K) \cong C_p \times C_p$. Los $p+1$ campos de grado p sobre K contenidos en \mathcal{K}_p son: $K(y + \beta_i)$, $1 \leq i \leq p$ y K_p , donde $\{\beta_i\}_{i=1}^p$ es una base de \mathbb{F}_{q^p} sobre \mathbb{F}_q . Por la Proposición 12.2.5, la única tal extensión de tal forma que \mathfrak{p}_∞ es no inerte es la extensión $K(w)$ que satisface $w^p - w = \alpha - f(T)$. Por lo tanto $E = K(w)$.

Si χ es el caracter asociado a E , $\chi = \chi_{P_1} \cdots \chi_{P_r}$ y el campo asociado a χ_{P_i} es $K(y_i)$, donde $y_i^p - y_i = \alpha_i := \frac{Q_i}{P_i^{e_i}}$, $1 \leq i \leq r$. Por lo tanto

$$E\mathbf{ge} = K(y_1, \dots, y_r). \quad (12.24)$$

Así $\mathcal{K}\mathbf{ge} = E\mathbf{ge}\mathcal{K} = K(y_1, \dots, y_r, \beta)$ con $\beta^p - \beta \notin \wp(\mathbb{F}_q)$.

Caso 2: Ahora consideramos el caso donde \mathfrak{p}_∞ es ramificado en \mathcal{K} . Sea $\mathcal{K}_1 := K(\beta)$, $\beta^p - \beta = f(T)$, $p \nmid \text{gr } f$. Sea $E := K(w)$ donde $w^p - w = \alpha - f(T) = \alpha_1 = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}}$. Por el Caso 1, $E\mathbf{ge} = K(y_1, \dots, y_r)$. Por lo tanto $\mathcal{K}\mathbf{ge} = E\mathbf{ge}\mathcal{K} = K(y_1, \dots, y_r, \beta)$.

Se ha probado:

Teorema 12.3.14. *Sea $\mathcal{K} = K(y)$ dado por (12.23). Entonces*

$$\mathcal{K}\mathbf{ge} = K(y_1, \dots, y_r, \beta),$$

donde $y_i^p - y_i = \frac{Q_i}{P_i^{e_i}}$, $1 \leq i \leq r$ y $\beta^p - \beta = f(T)$. □

Extensiones p -cíclicas

Este caso es similar al de extensiones de Artin-Schreier. Aquí consideramos $\mathcal{K} = K(\mathbf{y})$ donde $\mathbf{y}^p \dot{-} \mathbf{y} = \beta$, y la operación es la diferencia de Witt. La extensión es una p -extensión finita de grado menor o igual a p^n donde \mathbf{y} es de longitud n . Sean P_1, \dots, P_r los divisores primos finitos que son ramificados en \mathcal{K}/K .

Ahora sea $\mathbf{y}_i^p \dot{-} \mathbf{y}_i = \delta_i$, $1 \leq i \leq r$ y $\mathbf{z}^p \dot{-} \mathbf{z} = \mu$. Notemos que $K(\mathbf{y}, \mathbf{y}_i)$ y $K(\mathbf{y}, \mathbf{z})$ son extensiones no ramificadas de $K(\mathbf{y})$.

Por la Proposición 12.2.7, \mathfrak{p}_∞ se descompone totalmente $K(\mathbf{y} \dot{-} \mathbf{z})$, por lo tanto $E = K(\mathbf{y} \dot{-} \mathbf{z})$ está contenido en un campo de funciones ciclotómico $K(\Lambda_N)$.

Si χ es el caracter asociado a E , entonces $\chi = \chi_{P_1} \cdots \chi_{P_r}$, donde cada χ_{P_i} es de orden p^{n_i} con $n_i \leq n$. El campo asociado a χ_{P_i} es el campo contenido en un campo de funciones ciclotómico tal que P_i es el único primo ramificado y con el mismo comportamiento en su ramificación que el de P_i en E/K . Puesto

que en ambos casos la ramificación está completamente determinada por δ_i se sigue que el campo asociado a χ_{P_i} es $K(\mathbf{y}_i)$. Por lo tanto $E\mathfrak{ge} = K(\mathbf{y}_1, \dots, \mathbf{y}_r)$ puesto que \mathfrak{p}_∞ se descompone totalmente.

Notemos que $\mathcal{K}K(\mathbf{z})/\mathcal{K}$ es no ramificado y $S_\infty(\mathcal{K})$ se descompone totalmente. Se sigue de los Teoremas 12.3.8 y 12.3.10 que $\mathcal{K}\mathfrak{ge} = E\mathfrak{ge}K(\mathbf{z})$.

Por lo tanto hemos probado

Teorema 12.3.15. *Si \mathcal{K}/K está dado como en el Teorema 12.2.6, entonces*

$$\mathcal{K}\mathfrak{ge} = K(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z})$$

donde $\mathbf{y}_i^p \dot{-} \mathbf{y}_i = \delta_i$, $1 \leq i \leq r$ y $\mathbf{z}^p \dot{-} \mathbf{z} = \mu$. □

Ejemplo 12.3.16. Sea $K = \mathbb{F}_3(T)$ y $\mathcal{K} = K(\mathbf{y})$ donde $\mathbf{y}^3 \dot{-} \mathbf{y} = \beta = (\frac{1}{T} + 1, \frac{1}{T+1} + T)$. Entonces la descomposición prescrita en el Teorema 12.2.6 es:

$$\beta = \left(\frac{1}{T}, \frac{T+1}{T^2}\right) \dot{+} \left(0, \frac{1}{T+1}\right) \dot{+} (1, T).$$

Por lo tanto, si $\mathbf{y}_1^3 \dot{-} \mathbf{y}_1 = \delta_1 = (\frac{1}{T}, \frac{T+1}{T^2})$, $\mathbf{y}_2^3 \dot{-} \mathbf{y}_2 = \delta_2 = (0, \frac{1}{T+1})$ y $\mathbf{z}^3 \dot{-} \mathbf{z} = \mu = (1, T)$, entonces $\mathcal{K}\mathfrak{ge} = K(\mathbf{y}_1, \mathbf{y}_2, \mathbf{z})$.

Teoría de Iwasawa

Este capítulo presenta el inicio de la Teoría de Iwasawa que fue desarrollada por Kenkichi Iwasawa, especialmente en [32, 34, 35]. El desarrollo que aquí presentamos está basado fuertemente en [75, Capítulo 13].

13.1. Campos ciclotómicos infinitos

Sea p un número primo en \mathbb{Z} y sea $\mathbb{Q}(\zeta_{p^\infty}) := \bigcup_{n=0}^{\infty} \mathbb{Q}(\zeta_{p^n})$. Sea $G := \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$. Se tiene que $\sigma \in G$ está determinado por su acción en ζ_{p^n} , $n \geq 1$. Sea $\sigma\zeta_{p^n} = \zeta_{p^n}^{a_n}$ con $a_n \bmod p^n \in (\mathbb{Z}/p^n\mathbb{Z})^* = U_{p^n}$. Se tiene que $a_n \equiv a_{n-1} \bmod p^{n-1}$ por lo que obtenemos un elemento $(a_n)_{n \in \mathbb{N}} \in \mathbb{Z}_p^* = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^* = \varprojlim \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$. Recíprocamente, si $a \in \mathbb{Z}_p^*$, $\sigma\zeta_{p^n} = \zeta_{p^n}^a$ da un automorfismo de $\mathbb{Q}(\zeta_{p^\infty})$.

Si $p > 2$, tenemos $\mathbb{Z}_p^* = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^* = \varprojlim (\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Si $p = 2$, $\mathbb{Z}_2^* = \varprojlim (\mathbb{Z}/2^n\mathbb{Z})^* = \varprojlim (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

$$\begin{array}{ccc}
 \mathbb{Q}(\zeta_p) & \xrightarrow{\mathbb{Z}_p} & \mathbb{Q}(\zeta_{p^\infty}) \\
 U_p \cong \downarrow & & \downarrow C_{p-1} \\
 \mathbb{Q} & \xrightarrow{\mathbb{Z}_p} & \mathbb{Q}_\infty
 \end{array}
 \quad p > 2
 \qquad
 \begin{array}{ccc}
 \mathbb{Q}(\zeta_4) & \xrightarrow{\mathbb{Z}_2} & \mathbb{Q}(\zeta_{2^\infty}) \\
 C_2 \downarrow & & \downarrow C_2 \\
 \mathbb{Q} & \xrightarrow{\mathbb{Z}_2} & \mathbb{Q}_\infty
 \end{array}$$

Estamos particularmente interesados en $\mathbb{Q}(\zeta_{p^\infty})$ y $\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{p^\infty})^{C_{p-1}}$, $p \geq 2$.

13.2. Ramificación en extensiones algebraicas

Aquí presentamos una teoría de ramificación para extensiones algebraicas arbitrarias.

Sea k/\mathbb{Q} una extensión algebraica no necesariamente finita. Sea $\mathcal{O}_k := \{\alpha \in k \mid \text{Irr}(\alpha, x, \mathbb{Q}) \in \mathbb{Z}[x]\}$. \mathcal{O}_k es el *anillo de enteros* de k . Se tiene

$$\mathcal{O}_k = \varinjlim_{\substack{[E:\mathbb{Q}] < \infty \\ E \subseteq k}} \mathcal{O}_E = \bigcup_{\substack{[E:\mathbb{Q}] < \infty \\ E \subseteq k}} \mathcal{O}_E.$$

Observación 13.2.1. En general \mathcal{O}_k no es noetheriano y por lo tanto no es dominio Dedekind. Más adelante daremos un ejemplo.

Lo que si tenemos es:

Proposición 13.2.2. Si \mathfrak{p} es un ideal primo no cero de \mathcal{O}_k , entonces \mathfrak{p} es maximal.

Demostración. Se tiene que $\mathcal{O}_k/\mathfrak{p}$ es un dominio entero tal que si $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo de \mathbb{Z} . Sea $\alpha \in \mathfrak{p}$, $\alpha \neq 0$. Entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ y $0 \neq N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\alpha \in \mathfrak{p} \cap \mathbb{Z}$, es decir, $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$. Por lo tanto $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ con p un número primo. Se tiene

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} \cong (\mathfrak{p} + \mathbb{Z})/\mathfrak{p} \subseteq \mathcal{O}_k/\mathfrak{p}.$$

Por otro lado si $\bar{\beta} \in \mathcal{O}_k/\mathfrak{p}$, $\beta \in \mathcal{O}_k$, β entero sobre \mathbb{Z} , por lo tanto $\bar{\beta}$ es algebraico sobre \mathbb{F}_p lo cual implica que $\mathcal{O}_k/\mathfrak{p} \subseteq \overline{\mathbb{F}_p}$. Es decir, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \subseteq \mathcal{O}_k/\mathfrak{p} \subseteq \overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

Ahora veamos que $\mathcal{O}_k/\mathfrak{p}$ es un campo. Si $\bar{\alpha} \in \mathcal{O}_k/\mathfrak{p}$, $\bar{\alpha} \neq 0$, $\bar{\alpha} \in \overline{\mathbb{F}_p}$ y $\bar{\alpha}$ satisface una ecuación

$$\bar{\alpha}^n + a_{n-1}\bar{\alpha}^{n-1} + \cdots + a_1\bar{\alpha} + a_0 = 0$$

con $a_i \in \mathbb{F}_p$ y $a_0 \neq 0$. Por tanto

$$-a_0^{-1}(\bar{\alpha}^{n-1} + \cdots + a_2\bar{\alpha} + a_1)\bar{\alpha} = 1$$

es decir $\bar{\alpha}^{-1} = -a_0^{-1}(\bar{\alpha}^{n-1} + \cdots + a_2\bar{\alpha} + a_1) \in \mathcal{O}_k/\mathfrak{p}$ y $\bar{\alpha}$ es invertible. Por lo tanto $\mathcal{O}_k/\mathfrak{p}$ es un campo y \mathfrak{p} es maximal. \square

Corolario 13.2.3. $\mathcal{O}_k/\mathfrak{p}$ es una extensión abeliana de \mathbb{F}_p .

Demostración. Se sigue de que $\mathbb{F}_p \subseteq \mathcal{O}_k/\mathfrak{p} \subseteq \overline{\mathbb{F}_p}$ y de que

$$\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \text{Gal}\left(\varinjlim \mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \varprojlim \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z}) \cong \hat{\mathbb{Z}}$$

el cual es abeliano. \square

Más generalmente, tenemos

Corolario 13.2.4. *Si L/K es una extensión algebraica cualquiera de campos numéricos, entonces si \mathfrak{P} es un ideal primo no cero de \mathcal{O}_L , $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ es un ideal primo no cero de K y $\mathcal{O}_L/\mathfrak{P}$ es una extensión de Galois abeliana de $\mathcal{O}_K/\mathfrak{p}$.*

Demostración. Se sigue de que $\mathbb{F}_p \subseteq \mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P} \subseteq \overline{\mathbb{F}_p}$. □

Recíprocamente, tenemos:

Proposición 13.2.5. *Sea L/K una extensión algebraica de campos. Si \mathfrak{p} es un ideal no cero de \mathcal{O}_K , existe un ideal primo \mathfrak{P} de \mathcal{O}_L tal que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.*

Demostración. Primero veamos que $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. Se tiene que la localización $(\mathcal{O}_L)_{\mathfrak{p}} = \{ \frac{a}{b} \mid a \in \mathcal{O}_L, b \in \mathcal{O}_K \setminus \mathfrak{p} \}$ es un anillo entero sobre $(\mathcal{O}_K)_{\mathfrak{p}}$ y $(\mathcal{O}_K)_{\mathfrak{p}}$ es un anillo local con ideal máximo $\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$. Si $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ se tendría que $\mathfrak{p}(\mathcal{O}_L)_{\mathfrak{p}} = (\mathcal{O}_L)_{\mathfrak{p}}$ y en este caso tendríamos

$$1 = a_1 b_1 + \cdots + a_n b_n \quad \text{con} \quad a_i \in \mathfrak{p}, b_i \in (\mathcal{O}_L)_{\mathfrak{p}}.$$

Sea $B = (\mathcal{O}_K)_{\mathfrak{p}}[b_1, \dots, b_n]$. Se tiene $\mathfrak{p}B = B$ y B es un $A := (\mathcal{O}_K)_{\mathfrak{p}}$ módulo finitamente generado pues cada b_i es entero sobre A . Por el Lema de Nakayama (Teorema 13.2.6 más adelante), se sigue que $B = 0$ lo cual es absurdo. Por tanto $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.

Se tiene el diagrama

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & (\mathcal{O}_L)_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ \mathcal{O}_K & \longrightarrow & (\mathcal{O}_K)_{\mathfrak{p}} \end{array}$$

$\mathfrak{p}(\mathcal{O}_L)_{\mathfrak{p}} \subseteq \mathfrak{m}(\mathcal{O}_L)_{\mathfrak{p}}$ con \mathfrak{m} es un ideal maximal. En particular $\mathfrak{m} \cap (\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$. Por tanto $\mathfrak{m}' := \mathfrak{m} \cap \mathcal{O}_L$ es un ideal primo de \mathcal{O}_L y se tiene

$$\mathfrak{m}' \cap \mathcal{O}_K = \mathfrak{m}(\mathcal{O}_L)_{\mathfrak{p}} \cap (\mathcal{O}_K)_{\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}(\mathcal{O}_L)_{\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}. \quad \square$$

Teorema 13.2.6 (Lema de Nakayama). *Sea A un anillo conmutativo con unidad y sea $\mathfrak{a} \subseteq \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$. Si M es un A -módulo finitamente generado tal que $\mathfrak{a}M = M$ entonces $M = 0$.*

Demostración. Supongamos que $M \neq 0$ y sea m el mínimo número de generadores de M como A -módulo. Digamos que $M = A\omega_1 + \cdots + A\omega_m$. Se tiene que $\omega_1 = a_1\omega_1 + \cdots + a_m\omega_m$ para algunos $a_i \in \mathfrak{a}$. Por tanto $(1 - a_1)\omega_1 = a_2\omega_2 + \cdots + a_m\omega_m$.

Ahora $1 - a_1 \in A^*$ pues en caso contrario existiría \mathfrak{m} maximal tal que $1 - a_1 \in \mathfrak{m}$ pero $a_1 \in \mathfrak{a} \subseteq \mathfrak{m}$ implicaría $1 \in \mathfrak{m}$. Por tanto $\omega_1 \in \langle \omega_2, \dots, \omega_m \rangle$ y en este caso M está generado por $m - 1$ elementos lo cual es absurdo. Por tanto $M = 0$. \square

Como en el caso finito, tenemos la transitividad sobre los ideales primos que se encuentran sobre uno dado del campo base, es decir:

Proposición 13.2.7. *Sea L/K una extensión de Galois de campos numéricos. Sean \mathfrak{P} y \mathfrak{P}' dos ideales primos de \mathcal{O}_L sobre el ideal primo \mathfrak{p} de \mathcal{O}_K . Entonces existe $\sigma \in \text{Gal}(L/K)$ tal que $\sigma\mathfrak{P} = \mathfrak{P}'$.*

Demostración. Este resultado lo conocemos cuando la extensión L/K es finita. Sean

$$K = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \dots \subseteq L, \quad L = \bigcup_{n=1}^{\infty} F_n$$

lo cual es posible hacerlo pues L es un conjunto numerable, tal que F_n/K son extensiones finitas de Galois. Sean $\mathfrak{p}_n := \mathfrak{P} \cap \mathcal{O}_{F_n}$, $\mathfrak{p}'_n := \mathfrak{P}' \cap \mathcal{O}_{F_n}$. Existe $\tau_n \in \text{Gal}(F_n/K)$ tal que $\tau_n(\mathfrak{p}_n) = \mathfrak{p}'_n$. Sean $\sigma_n \in \text{Gal}(L/K)$ tal que $\sigma_n|_{F_n} = \tau_n$. Puesto que $\text{Gal}(L/K)$ es compacto, la sucesión $\{\sigma_n\}_{n=1}^{\infty}$ tiene un punto de acumulación σ . Sea $\sigma_{n_i} \xrightarrow{i \rightarrow \infty} \sigma$. Por facilidad suponemos $\sigma_n \xrightarrow{n} \sigma$. Sea m arbitrario. Se tiene que $\text{Gal}(L/F_m)$ es una vecindad abierta de Id y $\sigma^{-1}\sigma_n \in \text{Gal}(L/F_m)$ para $n \gg m$. Por tanto para n suficientemente grande tenemos

$$\sigma^{-1}\sigma_n\mathfrak{p}_m = \mathfrak{p}_m. \quad \text{Por tanto} \quad \sigma\mathfrak{p}_m = \sigma_n\mathfrak{p}_m = \sigma_n(\mathfrak{p}_n \cap \mathcal{O}_{F_m}) = \mathfrak{p}'_n \cap \mathcal{O}_{F_m} = \mathfrak{p}'_m.$$

Puesto que $\mathfrak{P} = \bigcup_{m=1}^{\infty} \mathfrak{p}_m$ y $\mathfrak{P}' = \bigcup_{m=1}^{\infty} \mathfrak{p}'_m$ se sigue que $\sigma\mathfrak{P} = \mathfrak{P}'$. \square

Ejemplo 13.2.8. Este es un ejemplo de un anillo \mathcal{O}_K que no es dominio Dedekind. Sea $K = \mathbb{Q}(\zeta_{p^\infty})$ y sea $\mathfrak{p} = \bigcup_{n=1}^{\infty} \mathfrak{p}_n$ donde $\mathfrak{p}_n = \langle 1 - \zeta_{p^n} \rangle$ es el ideal primo sobre p de $\mathbb{Q}(\zeta_{p^n})$. Se tiene que $\langle 1 - \zeta_{p^n} \rangle$ es el ideal primo sobre p de $\mathbb{Q}(\zeta_{p^n})$ y $\langle 1 - \zeta_{p^n} \rangle^{\varphi(p^n)} = \langle p \rangle$. En particular $\mathfrak{p} = \langle 1 - \zeta_p, 1 - \zeta_{p^2}, \dots, 1 - \zeta_{p^n}, \dots \rangle$ y puesto que $\langle 1 - \zeta_{p^n} \rangle^p = \langle 1 - \zeta_{p^{n-1}} \rangle$ se sigue que $\mathfrak{p}^p = \mathfrak{p}$. Esto implica lo que queremos.

Otra forma de obtener lo mismo es notando que \mathfrak{p} no es finitamente generado pues si $\mathfrak{p} = \langle a_1, \dots, a_m \rangle$, entonces cada $a_i \in \mathfrak{p}_{t_i}$ para algún t_i . Sea $t := \max\{t_i \mid 1 \leq i \leq m\}$. Por tanto $a_1, \dots, a_m \in \mathfrak{p}_t = \langle 1 - \zeta_{p^t} \rangle$ pero esto es absurdo pues $1 - \zeta_{p^{t+1}} \notin \mathfrak{p}_t$.

El Ejemplo 13.2.8 nos indica, entre otras cosas, que no podemos estudiar ramificación vía la descomposición de primos. En su lugar lo hacemos usando los grupos de inercia. Esto lo hacemos como en el caso finito.

Definición 13.2.9.

Sea K/k una extensión de Galois. Sea \mathfrak{p} un primo de k y sea \mathfrak{P} un primo de L sobre \mathfrak{p} . Se define el *grupo de descomposición* de \mathfrak{P} sobre \mathfrak{p} por $D(\mathfrak{P}|\mathfrak{p}) = D = \{\sigma \in \text{Gal}(K/k) \mid \sigma\mathfrak{P} = \mathfrak{P}\}$. El *grupo de inercia* de \mathfrak{P} sobre \mathfrak{p} se define por $I(\mathfrak{P}|\mathfrak{p}) = I = \{\sigma \in D \mid \sigma\alpha \equiv \alpha \pmod{\mathfrak{P}} \forall \alpha \in \mathcal{O}_K\}$.

Proposición 13.2.10. *Se tiene que D y I son subgrupos cerrados de $G = \text{Gal}(K/k)$ y por tanto son compactos.*

Demostración. Sea $k = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \dots \subseteq K$ tal que $K = \bigcup_{n=1}^{\infty} F_n$ y F_n/k de Galois y finita. Sean $\mathfrak{P}_n := \mathfrak{P} \cap \mathcal{O}_{F_n}$, $D_n = \{\sigma \in G \mid \sigma\mathfrak{P}_n = \mathfrak{P}_n\}$. Se tiene que $\mathfrak{P} = \bigcup_{n=1}^{\infty} \mathfrak{P}_n$, $D \subseteq D_n$ y $D = \bigcap_{n=1}^{\infty} D_n$. Ahora bien, se tiene $\text{Gal}(K/F_n) \subseteq D_n$ y $\text{Gal}(K/F_n)$ es abierto por lo que D_n es abierto. Se sigue que D_n es cerrado por lo que D es cerrado.

Veamos que I es cerrado. Sea $\sigma \notin I$. Entonces existe $\alpha \in \mathcal{O}_K$ tal que $\sigma\alpha - \alpha \notin \mathfrak{P}$. Consideremos $\widehat{k(\alpha)/k}$ la cerradura de Galois de $k(\alpha)/k$. Se tiene que $\widehat{k(\alpha)/k}$ es finita y $N := \text{Gal}(K/\widehat{k(\alpha)/k})$ es un subgrupo abierto de G . Ahora bien σN es una vecindad abierta de σ . Sea $\psi \in N$. Entonces $\psi(\alpha) = \alpha$ por lo que $\sigma\psi(\alpha) = \sigma(\alpha)$ y $(\sigma\psi)(\alpha) - \alpha = \sigma\alpha - \alpha \notin \mathfrak{P}$. Por tanto $\sigma N \cap I = \emptyset$ de donde se sigue que el complemento de I es abierto y por tanto I es cerrado. \square

Sea $\varphi: D \rightarrow \text{Gal}(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}) =: G(\mathfrak{P})$ el mapeo natural, es decir, si $\sigma \in D$, $\sigma\mathcal{O}_K = \mathcal{O}_K$, $\sigma\mathfrak{P} = \mathfrak{P}$ y $\sigma|_{\mathcal{O}_K} = \text{Id}_{\mathcal{O}_K}$ por lo que $\tilde{\sigma}: \mathcal{O}_K/\mathfrak{P} \rightarrow \mathcal{O}_K/\mathfrak{P}$, $\sigma(x \pmod{\mathfrak{P}}) = \sigma x \pmod{\mathfrak{P}}$ está bien definida y $\tilde{\sigma} \in G(\mathfrak{P})$. Entonces $\varphi(\sigma) = \tilde{\sigma}$. Se tiene:

Teorema 13.2.11. *La sucesión $1 \rightarrow I \rightarrow D \xrightarrow{\varphi} G(\mathfrak{P}) \rightarrow 1$ es exacta.*

Demostración. Sabemos que en el caso finito, φ es suprayectiva. Ahora $G(\mathfrak{P}) = \varprojlim \text{Gal}(\mathcal{O}_{F_n}/\mathfrak{P}_n/\mathcal{O}_k/\mathfrak{p})$. Sea $\tilde{D}_n := D(\mathfrak{P}_n|\mathfrak{p}) \subseteq \text{Gal}(F_n/k)$. Se tiene $D = \varprojlim \tilde{D}_n$ bajo los mapeos:

$$\begin{aligned} \varphi: D &\longrightarrow \prod_{n=1}^{\infty} \tilde{D}_n \subseteq \prod_{n=1}^{\infty} \text{Gal}(F_n/k) \\ \sigma &\longmapsto \prod_{n=1}^{\infty} \sigma|_{F_n}, \quad \sigma|_{F_n} \in \text{Gal}(F_n/k) \end{aligned}$$

$\sigma|_{F_n}(\mathfrak{P}_n) = \sigma(\mathfrak{P} \cap \mathcal{O}_{F_n}) = \mathfrak{P} \cap \mathcal{O}_{F_n} = \mathfrak{P}_n$. Entonces tenemos el diagrama conmutativo

$$\begin{array}{ccc}
\tilde{D}_n & \xrightarrow{\varphi_n} & \text{Gal}((\mathcal{O}_{F_n}/\mathfrak{P}_n)/(\mathcal{O}_k/\mathfrak{p})) \\
\uparrow & & \uparrow \\
\tilde{D}_{n+1} & \xrightarrow{\varphi_{n+1}} & \text{Gal}((\mathcal{O}_{F_{n+1}}/\mathfrak{P}_{n+1})/(\mathcal{O}_k/\mathfrak{p}))
\end{array}$$

donde las flechas verticales son los mapeos de restricción.

Ahora bien puesto que los mapeos φ_n son suprayectivos, pasando al límite, se sigue que φ es suprayectiva y por definición tenemos que $\text{núc } \varphi = I$. \square

Corolario 13.2.12. *Se tiene $D/I \cong \text{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p}))$.* \square

$$\begin{array}{ccc}
\overline{\mathbb{Q}} & \text{---} & \mathfrak{B} \\
\downarrow & & \downarrow \\
K & \text{---} & \mathfrak{P} \\
\downarrow & & \downarrow \\
k & \text{---} & \mathfrak{p}
\end{array}$$

Ahora supongamos que K/k es algebraica pero no necesariamente de Galois. Fijemos una cerradura algebraica $\overline{\mathbb{Q}}$ de \mathbb{Q} . Entonces $\overline{\mathbb{Q}}/K$ y $\overline{\mathbb{Q}}/k$ son extensiones de Galois. Sean \mathfrak{P} y \mathfrak{p} como antes y sea \mathfrak{B} un primo $\mathcal{O}_{\overline{\mathbb{Q}}}$ tal que $\mathfrak{B}|_K = \mathfrak{P}$. Entonces

$$\begin{aligned}
I(\mathfrak{B}|\mathfrak{p}) &\subseteq \text{Gal}(\overline{\mathbb{Q}}/k), \\
I(\mathfrak{B}|\mathfrak{P}) &\subseteq \text{Gal}(\overline{\mathbb{Q}}/K) \subseteq \text{Gal}(\overline{\mathbb{Q}}/k), \\
I(\mathfrak{B}|\mathfrak{P}) &= I(\mathfrak{B}|\mathfrak{p}) \cap \text{Gal}(\overline{\mathbb{Q}}/K).
\end{aligned}$$

Definición 13.2.13. Se define el *índice de ramificación* $e(\mathfrak{P}|\mathfrak{p})$ por: $e(\mathfrak{P}|\mathfrak{p}) = [I(\mathfrak{B}|\mathfrak{p}) : I(\mathfrak{B}|\mathfrak{P})]$ el cual puede ser infinito.

Observación 13.2.14. $e(\mathfrak{P}|\mathfrak{p})$ no depende de \mathfrak{B} pues si \mathfrak{B}' es otro primo de $\overline{\mathbb{Q}}$ sobre \mathfrak{P} , entonces existe $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$ tal que $\mathfrak{B}' = \sigma\mathfrak{B}$ y por tanto $I(\mathfrak{B}'|\mathfrak{p}) = \sigma I(\mathfrak{B}|\mathfrak{p})\sigma^{-1}$ y $I(\mathfrak{B}'|\mathfrak{P}) = \sigma I(\mathfrak{B}|\mathfrak{P})\sigma^{-1}$ y por lo tanto

$$[I(\mathfrak{B}'|\mathfrak{p}) : I(\mathfrak{B}'|\mathfrak{P})] = [\sigma I(\mathfrak{B}|\mathfrak{p})\sigma^{-1} : \sigma I(\mathfrak{B}|\mathfrak{P})\sigma^{-1}] = [I(\mathfrak{B}|\mathfrak{p}) : I(\mathfrak{B}|\mathfrak{P})].$$

En el caso en que K/k sea una extensión de Galois, la restricción

$$\begin{aligned}
\text{Gal}(\overline{\mathbb{Q}}/k) &\longrightarrow \text{Gal}(K/k) \\
\sigma &\longmapsto \sigma|_K
\end{aligned}$$

tiene como núcleo a $\text{Gal}(\overline{\mathbb{Q}}/K)$ y $I(\mathfrak{B}|\mathfrak{p}) \longrightarrow I(\mathfrak{P}|\mathfrak{p})$ es suprayectiva con núcleo $I(\mathfrak{B}|\mathfrak{P})$, es decir

$$\frac{I(\mathfrak{B}|\mathfrak{p})}{I(\mathfrak{B}|\mathfrak{P})} \cong I(\mathfrak{P}|\mathfrak{p}) \quad \text{y} \quad e(\mathfrak{P}|\mathfrak{p}) = |I(\mathfrak{P}|\mathfrak{p})|.$$

En el caso de lugares arquimideanos o infinitos, procedemos de la siguiente forma:

Definición 13.2.15. Un *lugar arquimideano* de k o un *lugar infinito* de k es, ya sea un encaje real $\phi: k \rightarrow \mathbb{R}$ o bien un par $(\psi, \bar{\psi})$ de encajes complejos $\psi, \bar{\psi}: k \rightarrow \mathbb{C}$, $\psi \neq \bar{\psi}$.

Por el Lema de Zorn, tenemos que cualquier encaje ϕ o $(\psi, \bar{\psi})$ se puede extender a un encaje: $\bar{\mathbb{Q}} \rightarrow \mathbb{C}$ y en particular se puede extender a un encaje de $K: K \rightarrow \mathbb{C}$.

Sea K/k una extensión de Galois y sean ϕ_1, ϕ_2 dos extensiones a K de un encaje ϕ de k . Entonces $\phi_2^{-1} \circ \phi_1 \in \text{Gal}(K/k)$ y por tanto $\phi_1 = \phi_2 \sigma$ para algún $\sigma \in \text{Gal}(K/k)$. Similarmente, si $(\psi_1, \bar{\psi}_1)$ y $(\psi_2, \bar{\psi}_2)$ son dos extensiones de ϕ , $\psi_1 = \psi_2 \sigma$ y $(\psi_1, \bar{\psi}_1) = (\psi_2, \bar{\psi}_2) \circ \sigma = (\psi_2 \circ \sigma, \bar{\psi}_2 \circ \sigma)$.

De manera análoga si $(\psi_1, \bar{\psi}_1)$ y $(\psi_2, \bar{\psi}_2)$ se pueden extender a $(\psi, \bar{\psi})$, entonces $\psi_2^{-1} \psi_1 \in \text{Gal}(K/k)$ y $\psi_1 = \psi_2 \sigma$, $\bar{\psi}_1 = \bar{\psi}_2 \sigma$.

Si w es un lugar arquimideano de K , $w|_k = v$ es un lugar arquimideano de k y se define el grupo de inercia y el grupo de descomposición de w sobre v por:

Definición 13.2.16. Sea K/k una extensión de Galois. Entonces se define

$$I(w|v) = D(w|v) = \{\sigma \in \text{Gal}(K/k) \mid w\sigma = w\}.$$

Si w es real, $w\sigma = w$ implica $\sigma = w^{-1}w = \text{Id}$.

Si w es complejo, $w = (\psi, \bar{\psi})$ y $(\psi, \bar{\psi})\sigma = (\psi, \bar{\psi})$ entonces $\psi\sigma = \psi$ o $\bar{\psi}\sigma = \psi$, es decir, $\sigma = \text{Id}$ o $\sigma = \bar{\psi}^{-1} \circ \psi$. Si $v = (\phi, \bar{\phi})$ es complejo, $\text{Id} = \sigma|_k = \bar{\psi} \circ \psi|_k = \bar{\phi}^{-1} \circ \phi \neq \text{Id}$ no es posible por lo que si v es complejo, $\sigma = \text{Id}$. Si v es real, $\bar{\psi}^{-1} \circ \psi|_k = \phi^{-1} \circ \phi = \text{Id}$ por lo que existe $\bar{\psi}^{-1} \circ \psi = \psi^{-1} \circ \bar{\psi} = \sigma \neq \text{Id}$.

En resumen,

Teorema 13.2.17. Se tiene $|I(w, v)| = 1$ o 2 y $|I(w, v)| = 2 \iff v$ es real y w es complejo. En este último caso, si $w = (\psi, \bar{\psi})$, $I(w, v) = \{\text{Id}, \bar{\psi}^{-1} \circ \psi = \psi^{-1} \circ \bar{\psi}\}$. \square

13.3. Pro- p -grupos

Definición 13.3.1. Sea p un número primo. Un grupo profinito H se llama *pro- p -grupo* si H es el límite proyectivo de p -grupos finitos:

$$H = \varprojlim_N H/N, \quad [H : N] = p^n, \quad n \in \mathbb{N}, \quad N \triangleleft H.$$

Ejemplo 13.3.2. \mathbb{Z}_p es un pro- p -grupo (abeliano): $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Definición 13.3.3. Sea I un conjunto y sea $L(I)$ el grupo discreto libre generado por elementos x_i , $i \in I$. Sea X la familia de subgrupos normales M de $L(I)$ tales que:

- (I) $L(I)/M$ es un p -grupo finito.
- (II) M contiene a casi todo x_i , es decir, a todo x_i salvo un número finito.

Sea $F(I) := \varprojlim_{M \in X} L(I)/M$. Entonces el pro- p -grupo $F(I)$ se llama el pro- p -grupo libre generado por los x_i .

Ejemplo 13.3.4. Sea I finito, $|I| = n \in \mathbb{N} \cup \{0\}$. Ponemos $F(I) = F(n)$. Se tiene $F(0) = \{1\}$, $F(1) \cong \mathbb{Z}_p$ pues $L(1) = \mathbb{Z}$ y $F(1) = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$.

Proposición 13.3.5. Se tiene $F(n)/F'(n) \cong \mathbb{Z}_p^n$ y más generalmente, para I arbitrario, $F(I)/F'(I) \cong \bigoplus_{i \in I} \mathbb{Z}_p$.

Demostración. (Esquema). Se tiene

$$F(I) = \varprojlim L(I)/H, \quad F'(I) = \varprojlim L'(I)/(H \cap L'(I))$$

y se tiene $L'(I)/(H \cap L'(I)) \cong HL'(I)/H$, por lo que

$$\begin{aligned} \frac{L(I)/H}{L'(I)/(H \cap L'(I))} &\cong \frac{L(I)/H}{HL'(I)/H} = L(I)/HL'(I) = \left(\bigoplus_{i \in I} \mathbb{Z} \right) / H \quad \text{y} \\ \varprojlim_{i \in I} \left(\bigoplus_{i \in I} \mathbb{Z} \right) / H &\cong \bigoplus_{i \in I} \mathbb{Z}_p. \quad \square \end{aligned}$$

13.4. Extensiones \mathbb{Z}_p

Consideremos una cadena de campos

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq \dots \subseteq K_\infty = \bigcup_{n=0}^{\infty} K_n$$

tal que $\text{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Entonces $\text{Gal}(K_\infty/K) = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$.

Definición 13.4.1. En el desarrollo anterior, K_∞/K es una *extensión* \mathbb{Z}_p o una *extensión* Γ donde ponemos $\Gamma := \mathbb{Z}_p$.

Ejemplo 13.4.2 (Extensión p -ciclotómica de \mathbb{Q}). (Ver Teoremas 5.2.6, 5.2.7 y 5.2.8). Sea $K = \mathbb{Q}$. Se tiene que $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ tiene como grupo de Galois a $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong U_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^*$.

Primero consideremos $p > 2$. Entonces U_{p^n} es cíclico y se tiene $(\mathbb{Z}/p^n\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$ (Teorema 3.2.21).

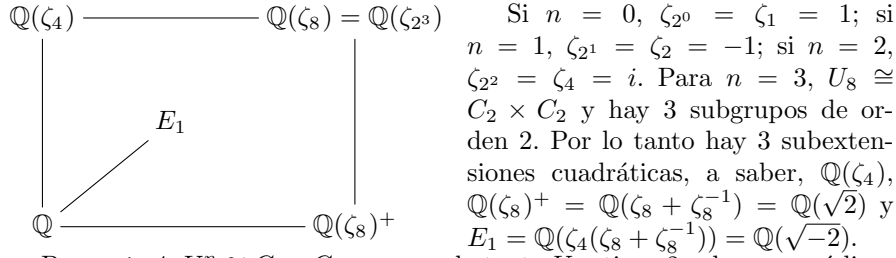
En particular U_{p^n} contiene un único subgrupo de orden $p-1$, a saber, $\mathbb{Z}/(p-1)\mathbb{Z}$ en la descomposición anterior. Sea $\mathbb{Q}_{n-1} := \mathbb{Q}(\zeta_{p^n})^{\mathbb{Z}/(p-1)\mathbb{Z}}$. Entonces $\text{Gal}(\mathbb{Q}_{n-1}/\mathbb{Q}) \cong \mathbb{Z}/(p^{n-1}\mathbb{Z})$.

Notemos que 2 divide a $p-1$ por lo que $\mathbb{Q}_{n-1} \subseteq \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1}) = \mathbb{Q}(\zeta_{p^n})^+ \subseteq \mathbb{R}$.

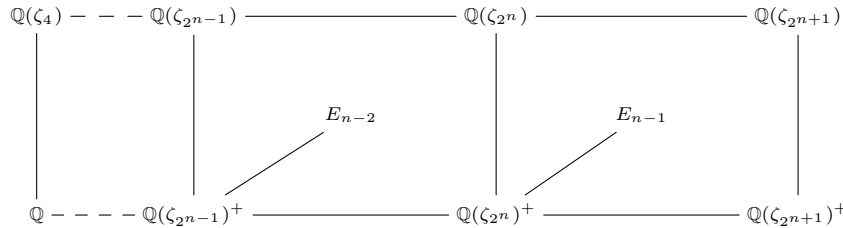
Sea $\mathbb{Q}_\infty := \bigcup_{n=1}^{\infty} \mathbb{Q}_n$. Entonces $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

Ahora si $p = 2$, tenemos para $n \geq 2$ que

$$\text{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}) \cong U_{2^n} \cong \langle \pm 1 \rangle \times \langle 1 + 2^2 \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z}).$$



Para $n \geq 4$, $U_{2^n} \cong C_2 \times C_{2^{n-2}}$ y por lo tanto U_{2^n} tiene 2 subgrupos cíclicos de orden 2^{n-2} y por lo tanto 2 grupos cociente cíclicos de orden 2^{n-2} .



Hay 3 subcampos de $\mathbb{Q}(\zeta_{2^n})$ de grado 2^{n-2} sobre \mathbb{Q} , 2 de ellos son cíclicos sobre \mathbb{Q} y el otro no (para $n \geq 4$). Los 3 subcampos son $\mathbb{Q}(\zeta_{2^{n-1}})$, $\mathbb{Q}(\zeta_{2^n})^+$ y $E_{n-2} = \mathbb{Q}(\zeta_4(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}))$. Puesto que $\mathbb{Q}(\zeta_{2^{n-1}})/\mathbb{Q}$ no es cíclico, $\mathbb{Q}(\zeta_{2^n})^+$ y E_{n-2} son las extensiones cíclicas de \mathbb{Q} de grado 2^{n-2} .

Se tiene que $E_{n-2} \not\subseteq E_{n-1}$ pues de lo contrario tendríamos que $\mathbb{Q}(\zeta_{2^n}) = E_{n-2}\mathbb{Q}(\zeta_{2^{n-1}})^+ \subseteq E_{n-1}$ lo cual es absurdo.

Ahora bien $\mathbb{Q}(\zeta_{2^n})^+$ corresponde al subgrupo $\{\pm 1\}$ de U_{2^n} , es decir, $\mathbb{Q}(\zeta_{2^n})^+ = \mathbb{Q}(\zeta_{2^n})^{\{\pm 1\}}$ y $\text{Gal}(\mathbb{Q}(\zeta_{2^n})^+/\mathbb{Q}) \cong U_n/\{\pm 1\} \cong \langle 1 + 2^2 \rangle \cong C_{2^{n-2}}$.

En particular $\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})^+ = \mathbb{Q}(\zeta_{2^\infty})^+$ satisface:

$$\text{Gal}(\mathbb{Q}(\zeta_{2^\infty})^+/\mathbb{Q}) \cong \varprojlim_n C_{2^{n-2}} \cong \mathbb{Z}_2.$$

Ponemos $\mathbb{Q}_\infty := \mathbb{Q}(\zeta_{2^\infty})^+$.

Observación 13.4.3. Tenemos que para cualquier $p \geq 2$, \mathbb{Q}_∞ es la única extensión de \mathbb{Q} tal que $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

Para ver esto, sea K/\mathbb{Q} tal que $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p$, $p \geq 2$. Si $K \subseteq \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta_{p^\infty})$, el resultado se sigue del hecho de que $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \begin{cases} C_2 \times \mathbb{Z}_2 & \text{si } p = 2 \\ C_{p-1} \times \mathbb{Z}_p & \text{si } p \geq 3 \end{cases}$ y el único subgrupo finito de $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ es C_2 si $p = 2$ y C_{p-1} si $p \geq 3$.

Ahora bien, en general, sea $p^n \mathbb{Z}_p < \mathbb{Z}_p \cong \text{Gal}(K/\mathbb{Q})$ y sea $K_n := K^{p^n \mathbb{Z}_p}$, $\text{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}_p/p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n \mathbb{Z}$.

Por el Teorema de Kronecker–Weber, de hecho por el Teorema 4.2.4, $K \subseteq \mathbb{Q}(\zeta_{p^{n+1}})$ y por tanto $K = \bigcup_{n=1}^{\infty} K_n \subseteq \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^\infty})$ y se sigue la unicidad.

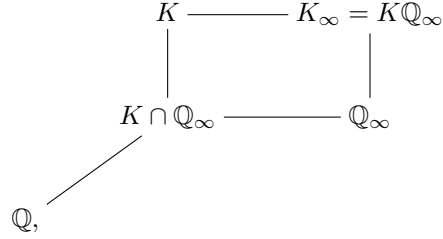
Veamos con más detalle $\mathbb{Q}(\zeta_{2^\infty})^+ = \mathbb{Q}(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1})$. Sea $\alpha_n := \zeta_{2^n} + \zeta_{2^n}^{-1}$. Entonces

$$\begin{aligned} \alpha_0 &= \zeta_1 + \zeta_1^{-1} = 1 + 1 = 2, \\ \alpha_1 &= \zeta_2 + \zeta_2^{-1} = -1 - 1 = -2, \\ \alpha_2 &= \zeta_4 + \zeta_4^{-1} = i + \frac{1}{i} = 0, \\ \alpha_3 &= \zeta_8 + \zeta_8^{-1}. \end{aligned}$$

Notemos que para $n \geq 3$, $\alpha_n^2 = (\zeta_{2^n} + \zeta_{2^n}^{-1})^2 = \zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1} + 2 = \alpha_{n-1} + 2$. Además $\alpha_n \geq 0$, por lo que $\alpha_n = \sqrt{\alpha_{n-1} + 2}$, esto es, $\alpha_3 = \sqrt{2}$, $\alpha_4 = \sqrt{2 + \sqrt{2}}$

$$\text{y en general } \alpha_n = \sqrt{\underbrace{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}}_{n-2}}.$$

Definición 13.4.4. Para todo primo $p \geq 2$, la extensión $\mathbb{Q}_\infty \subseteq \mathbb{Q}(\zeta_{p^\infty})$ que satisface $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ se le llama *la \mathbb{Z}_p -extensión ciclotómica* de \mathbb{Q} . Notemos que $\mathbb{Q}_\infty \subseteq \mathbb{R}$, y por tanto, $\mathbb{Q}_\infty \subseteq \mathbb{Q}(\zeta_{p^\infty})^+ = \mathbb{Q}(\zeta_{p^\infty}) \cap \mathbb{R}$.



Ahora sea K cualquier campo numérico finito, es decir, $[K : \mathbb{Q}] < \infty$. Sea $K_\infty := K\mathbb{Q}_\infty$. Se tiene que $\text{Gal}(K_\infty/K) \cong \text{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty) \subseteq \mathbb{Z}_p$. Por tanto $\text{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty) \cong p^n \mathbb{Z}_p$ para algún $n \geq 0$ y en particular $\text{Gal}(K_\infty/K) \cong p^n \mathbb{Z}_p \cong \mathbb{Z}_p$, es decir K_∞/K es una extensión \mathbb{Z}_p .

Definición 13.4.5. Esta extensión K_∞/K se llama la \mathbb{Z}_p extensión ciclotómica de K .

Observación 13.4.6. Sea $p \geq 2$ un número primo cualquiera. Entonces $\mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p)$ si $p > 2$ y $\text{Gal}(\mathbb{Q}(\zeta_{2p})/\mathbb{Q}) \cong C_2$ si $p = 2$ o C_{p-1} si $p > 2$. Entonces

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_{2p}) & \xrightarrow{\mathbb{Z}_p} & \mathbb{Q}(\zeta_{p^\infty}) \\
C_{p-1} \circ C_2 \downarrow & & \downarrow C_{p-1} \circ C_2 \\
\mathbb{Q} & \xrightarrow{\mathbb{Z}_p} & \mathbb{Q}_\infty
\end{array}
\quad \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{2p})) \cong \mathbb{Z}_p.$$

Proposición 13.4.7. Sea K una extensión finita de \mathbb{Q} y K_∞ la \mathbb{Z}_p -extensión ciclotómica de K . Entonces $\zeta_{p^\infty} \in K_\infty \iff \zeta_{2p} \in K$ y en este caso $K_\infty = K(\zeta_{p^\infty})$.

Demostración. Primero, si $\zeta_{2p} \in K$, entonces $K_\infty = K\mathbb{Q}_\infty \supseteq \mathbb{Q}(\zeta_{2p})\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{p^\infty})$ por lo que $\zeta_{p^\infty} \in K$.

Recíprocamente, si $\zeta_{p^\infty} \in K_\infty = K\mathbb{Q}_\infty$ se obtiene $K_\infty = K(\zeta_{p^\infty})\mathbb{Q}_\infty = K(\zeta_{p^\infty})$. Se tiene que

$$\begin{array}{ccc}
K & \xrightarrow{\mathbb{Z}_p} & K_\infty = K\mathbb{Q}_\infty = K\mathbb{Q}(\zeta_{p^\infty}) \\
| & & | \\
K \cap \mathbb{Q}(\zeta_{p^\infty}) & \xrightarrow{\mathbb{Z}_p} & \mathbb{Q}(\zeta_{p^\infty}) \\
/ & & \\
\mathbb{Q} & &
\end{array}$$

$\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/(K \cap \mathbb{Q}(\zeta_{p^\infty}))) \cong \text{Gal}(K\mathbb{Q}_\infty/K) \cong \mathbb{Z}_p.$

De esta forma se sigue que $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong C_t \times \mathbb{Z}_p$ donde $t = 2$ si $p = 2$ y $t = p - 1$ para $p \geq 3$. Los subgrupos cerrados de $C_t \times \mathbb{Z}_p$ isomorfos a \mathbb{Z}_p son únicamente los grupos $p^n \mathbb{Z}_p$ y por tanto $K \cap \mathbb{Q}(\zeta_{p^\infty})$ corresponde a algún $p^n \mathbb{Z}_p$. Se sigue que $K \cap \mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}(\zeta_\infty)^{p^n \mathbb{Z}_p} = \mathbb{Q}(\zeta_{2p^{n+1}})$ lo cual implica que $\zeta_{2p} \in K$.

Como vimos, en este caso $K_\infty = K\mathbb{Q}_\infty = K\mathbb{Q}_\infty(\zeta_{2p}) = K\mathbb{Q}(\zeta_{p^\infty}) = K(\zeta_{p^\infty})$. \square

13.5. Ramificación y descomposición de primos en $\mathbb{Q}_\infty/\mathbb{Q}$

Sea ℓ un primo de \mathbb{Q} que sea ramificado en $\mathbb{Q}_\infty/\mathbb{Q}$. Entonces si I es un primo de \mathbb{Q}_∞ sobre ℓ , $I := I(\ell)$ es un subgrupo cerrado de $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ y por lo tanto $I = p^n \mathbb{Z}_p$ para algún $n \geq 0$ o $I = 0$. Puesto que ℓ es ramificado, $I \neq 0$ y por tanto

$$I \cong p^n \mathbb{Z}_p \cong \mathbb{Z}_p, \mathbb{Q}^I = \mathbb{Q}_n \quad \text{pues} \quad \mathbb{Z}_p/I = \mathbb{Z}_p/p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n \mathbb{Z} \cong \text{Gal}(\mathbb{Q}_n/\mathbb{Q}).$$

En particular ℓ es ramificado en $\mathbb{Q}_{n+1}/\mathbb{Q}_n$ pero el único primo ramificado en $\mathbb{Q}_{n+1}/\mathbb{Q}_n$ es p de donde se sigue que $\ell = p$. Por otro lado, p es totalmente ramificado y por lo tanto sólo hay un primo \mathfrak{p} en \mathbb{Q}_∞ sobre p y $I(\mathfrak{p}|p) = \mathbb{Z}_p = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

Ahora consideremos $\ell \neq p$. Sea f_n el grado de inercia de ℓ en $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$. Por facilidad estudiaremos el caso $p > 2$. El caso $p = 2$ es similar aunque técnicamente más complicado.

Tenemos (Teorema 5.2.2 o (Teorema 5.2.10)) que $f_n = o(\ell \bmod p^n)$, es decir $\ell^{f_n} \equiv 1 \bmod p^n$, con f_n mínimo con esta propiedad. Consideremos el diagrama

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & \xrightarrow{\tilde{f}_n} & \mathbb{Q}(\zeta_{p^{n+1}}) \\ f_1 \downarrow & \nearrow f_{n+1} & \downarrow f'_1 \\ \mathbb{Q} & \xrightarrow{\tilde{f}'_n} & \mathbb{Q}_n \end{array}$$

Puesto que $\text{mcd}(\tilde{f}_n, f_1) = 1$, entonces $\tilde{f}_n = \tilde{f}'_n$. Por otro lado se tiene que $f_{n+1} = f_1 \tilde{f}_n$. Además, $\tilde{f}_n | [\mathbb{Q}(\zeta_{p^{n+1}}) : \mathbb{Q}(\zeta_p)] = p^n$. Se tiene que $f_n \neq 1$ para algún n pues de lo contrario, si $f_n = 1$ para toda n , entonces $p^n | \ell - 1$ lo cual es absurdo pues $\ell \neq 1$. Sea $n_0 \in \mathbb{N}$ tal que $\ell^{f_{n_0}} \equiv 1 \bmod p^{n_0}$, $f_{n_0} > 1$. Si $\{f_n\}_{n=1}^\infty$ fuese acotada, digamos $f_n \leq M$, entonces $\ell^{f_n} - 1 \leq \ell^M - 1$ y existiría $m \in \mathbb{N}$ tal que $p^m \nmid \ell^{f_m} - 1$ lo cual es absurdo. Por tanto $f_n \xrightarrow{n \rightarrow \infty} \infty$.

Sea I un primo en $\mathbb{Q}(\zeta_{p^\infty})$ sobre ℓ y sea $D = D(I|\ell)$ el cual es cerrado en \mathbb{Z}_p lo cual implica que $D \cong p^n \mathbb{Z}_p$ para alguna $n \in \mathbb{N} \cup \{0\}$ o $D = 0$. Esto último no puede ocurrir pues por lo anterior ℓ no puede ser totalmente descompuesto.

Así $D \cong p^n \mathbb{Z}_p$, $n \geq 0$ y en particular $\mathbb{Q}_n = \mathbb{Q}^D$ y ℓ es totalmente inerte $\mathbb{Q}_\infty/\mathbb{Q}_n$ y ℓ es totalmente descompuesto en \mathbb{Q}_n/\mathbb{Q} .

Si ∞ es el primo infinito, $I = D = \{0\}$.

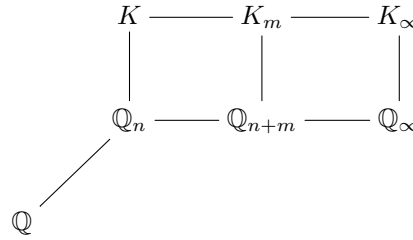
Observación 13.5.1. Esto último es otra demostración de que $\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{2^\infty})^+$ es la única extensión \mathbb{Z}_2 de \mathbb{Q} pues al no ser ∞ ramificado entonces se sigue que $\mathbb{Q}_\infty \subseteq \mathbb{R}$ y por tanto $\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{2^\infty})^+$.

Resumimos la discusión anterior en el siguiente resultado:

Teorema 13.5.2. Para $p \geq 2$, se tiene que p es el único primo (finito o infinito) que es ramificado en $\mathbb{Q}_\infty/\mathbb{Q}$ siendo además totalmente ramificado.

Para $\ell \neq p$, existe $n = n(\ell)$ tal que ℓ es totalmente descompuesto en $\mathbb{Q}_{n(\ell)}/\mathbb{Q}$ y totalmente inerte en $\mathbb{Q}_\infty/\mathbb{Q}_{n(\ell)}$. No hay primos finitos totalmente descompuestos en $\mathbb{Q}_\infty/\mathbb{Q}$. Finalmente el primo ∞ es totalmente descompuesto en $\mathbb{Q}_\infty/\mathbb{Q}$. \square

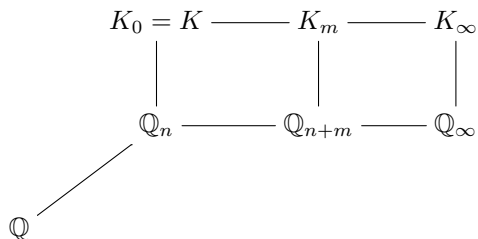
Sea ahora cualquier campo numérico finito y sea $K_\infty = K\mathbb{Q}_\infty$ la extensión \mathbb{Z}_p -ciclotómica de K . Sea $K \cap \mathbb{Q}_\infty = E$. Entonces $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}_\infty$ y $\text{Gal}(\mathbb{Q}_\infty/E)$ es un subgrupo cerrado de $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. En particular $\text{Gal}(\mathbb{Q}_\infty/E)$ es isomorfo a $p^n \mathbb{Z}_p$ para alguna $n \geq 0$ y por tanto $E = \mathbb{Q}_n$.



Puesto que K_∞/K es una extensión abeliana e infinita, por el Teorema de clase de Hilbert (Teorema 11.8.14), K_∞/K tiene necesariamente que ser ramificada. De hecho, si \mathfrak{p} es un primo en K sobre p , \mathfrak{p} es ramificado en K_∞/K .

Por otro lado, si \mathfrak{p} es cualquier primo de K ramificado en K_∞/K , entonces $\mathfrak{p}|_{\mathbb{Q}_n}$ es ramificado en \mathbb{Q}_∞ de donde, por el Teorema 13.5.2, se sigue que $\mathfrak{p}|_{\mathbb{Q}_n} = p$. Esto es, todos los p -primos de K son ramificados en K_∞/K y estos son los únicos.

Ahora, sea \mathfrak{l} primo de K tal que $\mathfrak{l}|_{\mathbb{Q}} = \ell \neq p$. Entonces el grado de inercia de ℓ en K_∞/\mathbb{Q}_n es ∞ de donde se sigue que si \mathfrak{l}_∞ es un primo de K_∞ sobre \mathfrak{l} , entonces $D(\mathfrak{l}_\infty|\mathfrak{l}) \cong p^m \mathbb{Z}_p$ para alguna $m \geq 0$. En otras palabras, \mathfrak{l} es totalmente descompuesto en K_m/K y totalmente inerte en K_∞/K_m . Los primos infinitos son totalmente descompuestos en K_∞/K .



Resumiendo tenemos:

Teorema 13.5.3. *Sea K un campo numérico finito y sea K_∞/K la extensión \mathbb{Z}_p -ciclotómica de K . Entonces los primos ramificados en K_∞/K son precisamente los primos sobre p . Si \mathfrak{l} no es un p -primo, entonces existe $m \in \mathbb{N} \cup \{0\}$ tal que \mathfrak{l} es totalmente descompuesto en K_m/K y totalmente inerte en K_∞/K_m .*

Finalmente los primos infinitos de K son totalmente descompuestos en K_∞/K . \square

A continuación enunciamos un teorema que corresponde a la teoría de campos locales.

Teorema 13.5.4. *Sea \mathbb{Q}_p el campo de los números p -ádicos. Sea K/k una extensión abeliana finita donde $[k : \mathbb{Q}_p] < \infty$. Entonces existe un mapeo, llamado el mapeo de reciprocidad de Artin*

$$\begin{aligned}
k^* &\longrightarrow \text{Gal}(K/k) \\
a &\longmapsto (a, K/k)
\end{aligned}$$

que induce un isomorfismo de grupos $k^/N_{K/k}K^* \cong \text{Gal}(K/k)$, donde $N_{K/k}$ es el mapeo norma.*

Sea I el subgrupo de inercia de $\text{Gal}(K/k)$. Entonces si U_k y U_K son los grupos de unidades de k y K respectivamente, se tiene $U_k/N_{K/k}U_K \cong I$.

Si K/k es no ramificada, entonces $\text{Gal}(K/k)$ es una extensión cíclica generada por el automorfismo de Frobenius F , $\langle F \rangle = \text{Gal}(\bar{K}/\bar{k})$, \bar{K} y \bar{k} los campos residuales y se tiene $(a, K/k) = F^{v_\pi(a)}$ donde v_π es la valuación de k , es decir, π es un elemento primo, esto es, un elemento de valuación 1. \square

Hasta ahora hemos considerado únicamente extensiones \mathbb{Z}_p -ciclotómicas K_∞/K , es decir, donde $K_\infty = K\mathbb{Q}_\infty$. Recordemos que \mathbb{Q} solo tiene una única extensión \mathbb{Z}_p y esta es la ciclotómica.

Cuando $K \neq \mathbb{Q}$, K puede tener otras extensiones \mathbb{Z}_p , de hecho, si K no es totalmente real, lo cual quiere decir que $r_1 \neq [K : \mathbb{Q}]$, K tiene más extensiones \mathbb{Z}_p . Algunos de los resultados que hemos obtenido para extensiones \mathbb{Z}_p -ciclotómicas siguen siendo ciertas para toda extensión \mathbb{Z}_p pero otros no.

Proposición 13.5.5. Sea K_∞/K una extensión \mathbb{Z}_p con K un campo numérico finito. Entonces para cada $n \geq 0$ hay un único subcampo K_n de grado p^n sobre K y K_n y K_∞ son los únicos subcampos entre K y K_∞ .

Demostración. Sea S un subgrupo cerrado de \mathbb{Z}_p y sea $x \in S$ tal que $v_p(x)$ sea mínimo. Entonces $x\mathbb{Z} \subseteq S$ y como S es cerrado, se sigue que $x\mathbb{Z}_p \subseteq S$. Ahora para $\xi \in S$, $v_p(\xi) \geq v_p(x)$, esto es, $\xi x^{-1} \in \mathbb{Z}_p$ y por tanto $S \subseteq x\mathbb{Z}_p$, de donde se sigue que $S = x\mathbb{Z}_p$. Ahora bien, claramente se tiene que $x\mathbb{Z}_p = 0$ o $p^n\mathbb{Z}_p$ para algún $n \geq 0$. Se sigue que los subcampos de la extensión K_∞/K son $K_\infty = K^{\{0\}}$ y $K_n = K_\infty^{p^n\mathbb{Z}_p}$, $K_0 = K$. \square

Teorema 13.5.6. Sea K_∞/K una extensión \mathbb{Z}_p con $[K : \mathbb{Q}] < \infty$. Sea \mathfrak{p} un divisor primo, posiblemente infinito, de K tal que $\mathfrak{p}|\mathbb{Q} \neq p$. Entonces \mathfrak{p} es no ramificado en K_∞/K , esto es, K_∞/K es no ramificada fuera de p .

Demostración. Sea $I \subseteq \text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ el grupo de inercia de \mathfrak{p} . Puesto que I es cerrado, entonces $I = \{0\}$ o $I = p^u\mathbb{Z}_p$ para algún $u \geq 0$. Si $I = \{0\}$, entonces \mathfrak{p} es no ramificado. Supongamos que $I = p^u\mathbb{Z}_p$, $u \geq 0$. En particular I es infinito. Para \mathfrak{p} un primo infinito, tenemos $|I| = 1$ o 2 , por lo que $\mathfrak{p}|\mathbb{Q} \neq \infty$. Ahora para cada n , sea \mathfrak{p}_n un primo en K_n tal que $\mathfrak{p}_n|_{K_{n-1}} = \mathfrak{p}_{n-1}$ y $\mathfrak{p}_n|_K = \mathfrak{p}|_{K_0} = \mathfrak{p}$. Sea \tilde{K}_n la completación de K_n en \mathfrak{p}_n y $\tilde{K}_\infty = \bigcup_{n=1}^{\infty} \tilde{K}_n$. Entonces $I \subseteq \text{Gal}(\tilde{K}_\infty/\tilde{K})$. Sea U el grupo de unidades de \tilde{K} .

Si I_n es el grupo de inercia de \mathfrak{p} en K_n/K , entonces se tiene que $I = \varprojlim_n I_n$.

Pero por teoría de campos de clase (Teorema 13.5.4) se tiene que $U_n \xrightarrow{\varphi_n} I_n$ es suprayectiva. Para cualquiera $n \leq m$, se tiene

$$\begin{array}{ccc} U & \xrightarrow{\varphi_n} & I_n \\ & \searrow \varphi_m & \nearrow \pi_{m,n} \\ & & I_m \end{array} \quad \pi_{m,n} \circ \varphi_m = \varphi_n,$$

entonces existe un epimorfismo continuo $U \rightarrow I = \varprojlim_n I_n \cong p^u\mathbb{Z}_p$.

Por otro lado $U \subseteq \mathcal{O}_{\tilde{K}}$, $[\tilde{K} : \mathbb{Q}_\ell] < \infty$ donde $\ell = \mathfrak{p}|\mathbb{Q} \neq p$. Sabemos que $\tilde{K}^* \cong \langle \pi \rangle \times U_{\tilde{K}} \cong \langle \pi \rangle \times \mu_{q-1} \times U_{\tilde{K}}^{(1)}$ donde π es un elemento primo, $|\mathcal{O}_{\tilde{K}}/\tilde{\mathfrak{p}}|$, $U_{\tilde{K}}^{(1)} = 1 + \tilde{\mathfrak{p}}$ y se tiene $U_{\tilde{K}} \supseteq U_{\tilde{K}}^{(1)} \supseteq \dots \supseteq U_{\tilde{K}}^{(m)} \supseteq \dots$, $U_{\tilde{K}}^{(m)} = 1 + \tilde{\mathfrak{p}}^m$, $U_{\tilde{K}}/U_{\tilde{K}}^{(1)} \cong (\mathcal{O}_{\tilde{K}}/\tilde{\mathfrak{p}})^* = K(\tilde{\mathfrak{p}})^*$ (campo residual) y $U_{\tilde{K}}^{(m)}/U_{\tilde{K}}^{(m+1)} \cong K(\tilde{\mathfrak{p}})$.

Si $e = e(\mathfrak{p}|\ell)$ en $\tilde{K}/\mathbb{Q}_\ell$, se tiene para $n > e/(\ell - 1)$ los isomorfismos y homeomorfismos, uno inverso del otro $\tilde{\mathfrak{p}}_K^n \xrightleftharpoons[\log]{\exp} U_K^{(n)}$.

Así se tiene que $\mathcal{O}_{\tilde{K}}/\tilde{\mathfrak{p}}_K$ es finito y $\mathcal{O}_{\tilde{K}} \cong \mathbb{Z}_\ell^r$ por lo que $\tilde{\mathfrak{p}}_K^m \cong \mathbb{Z}_\ell^r$. Por tanto $U_K^{(n)} \cong \mathbb{Z}_\ell^r$ y $U_{\tilde{K}}/U_{\tilde{K}}^{(n)}$ finito implica que

$$U_{\tilde{K}} \cong (\text{grupo finito}) \times \mathbb{Z}_\ell^r, \quad r = [\tilde{K} : \mathbb{Q}],$$

y el grupo finito es la torsión de $U_{\tilde{K}}$.

Se tiene que $U_{\tilde{K}} \rightarrow p^n \mathbb{Z}_p \cong \mathbb{Z}_p$ el cual no tiene torsión, por lo que existe un epimorfismo $\mathbb{Z}_\ell^r \rightarrow p^n \mathbb{Z}_p$ y por tanto

$$\mathbb{Z}_\ell^r \longrightarrow p^n \mathbb{Z}_p \xrightarrow{\pi} p^n \mathbb{Z}_p / p^{n+1} \mathbb{Z}_{p+1} \cong \mathbb{Z}/p\mathbb{Z}.$$

Sin embargo \mathbb{Z}_ℓ^r no tiene subgrupos de índice p pues $p \neq \ell$. Si sigue que $I = \{0\}$ y \mathfrak{p} no es ramificado en K_∞/K . \square

Proposición 13.5.7. *Sea $[K : \mathbb{Q}] < \infty$ y sea K_∞/K una extensión \mathbb{Z}_p . Existe al menos un primo ramificado en K_∞/K y existe $n \geq 0$ tal que todo primo ramificado en K_∞/K es totalmente ramificado en K_∞/K_n .*

Demostración. La máxima extensión abeliana no ramificada corresponde, por el Teorema de Clase de Hilbert (Teorema 11.8.14), al grupo de ideales de K y por tanto es finita. Siendo K_∞/K abeliana e infinita, necesariamente es ramificada.

Por el Teorema 13.5.6 sólo hay un número finito de ideales primos ramificados, a saber, a lo más los primos sobre p . Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ los primos ramificados, $r \geq 1$, y sean I_1, \dots, I_r los grupos de inercia respectivos. Se tiene $I_j \neq \{0\}$, $1 \leq i \leq r$, por lo que $I_j \cong p^{n_j} \mathbb{Z}_p$ para algún $n_j \geq 0$. En particular tenemos que $\bigcap_{j=1}^r I_j = p^m \mathbb{Z}_p$ donde $m = \max\{n_j \mid j = 1, \dots, r\}$. Por tanto, puesto que $K_m = K_\infty^{p^m \mathbb{Z}_p}$, se tiene que $\text{Gal}(K_\infty/K_m) \subseteq I_j$ y cada \mathfrak{p}_j es totalmente ramificado en K_∞/K_m . \square

Podemos dar otra demostración de la unicidad de \mathbb{Q}_∞ .

Corolario 13.5.8. $\mathbb{Q}_\infty/\mathbb{Q}$ es la única extensión \mathbb{Z}_p de \mathbb{Q} .

Demostración. Sea K_∞/\mathbb{Q} una extensión \mathbb{Z}_p de \mathbb{Q} . Tenemos que en K_∞/\mathbb{Q} únicamente p se ramifica y puesto que K_1/\mathbb{Q} es ramificada, se tiene que p es totalmente ramificado en K_∞/\mathbb{Q} .

Ahora bien, usando caracteres de Dirichlet deducimos que $K_n \subseteq \mathbb{Q}(\zeta_{p^{n_m}})$ para algún $n_m \in \mathbb{N}$ y además ∞ no es ramificado, lo cual implica que $K_n \subseteq \mathbb{Q}(\zeta_{p^{n_m}} + \zeta_{p^{n_m}}^{-1})$ de donde se sigue que $K_\infty = \bigcup_{n=1}^{\infty} K_n \subseteq \mathbb{Q}(\zeta_{p^\infty})^+$. Por lo tanto $K_n = \mathbb{Q}_n$ y $K_\infty = \mathbb{Q}_\infty$. \square

Se tiene que todo campo numérico finito K tiene al menos una extensión \mathbb{Z}_p , a saber, $K_\infty := K\mathbb{Q}_\infty$. Nos preguntamos ahora: dado un campo numérico K , $[K : \mathbb{Q}] < \infty$, ¿cuántas extensiones \mathbb{Z}_p tiene K ? Usamos la teoría de campos de clase para responder a esta pregunta.

Sea K dado, $[K : \mathbb{Q}] = d = r_1 + 2r_2 < \infty$ donde r_1 denota el número de encajes reales de $K \hookrightarrow \mathbb{R}$ y r_2 es el número de pares de encajes complejos no reales de K , $K \hookrightarrow \mathbb{C}$.

Sea U_K el grupo de unidades de K (más precisamente, de \mathcal{O}_K) y sea $E_1 = \{u \in U_K \mid u \equiv 1 \pmod{\mathfrak{p}} \text{ para toda } \mathfrak{p} \text{ de } K \text{ tal que } \mathfrak{p}|\mathbb{Q} = p\}$.

Sea $U_{K_p} = U_{\mathfrak{p}}$ el grupo de unidades del campo local K_p , π un elemento primo y $U_{1,\mathfrak{p}} = \{x \in U_{\mathfrak{p}} \mid x \equiv 1 \pmod{\mathfrak{p}}\}$. Sea $q = N\mathfrak{p}$, esto es, $q = |\mathcal{O}_{K_p}/\mathfrak{p}|$. Entonces $\mathcal{O}_{K_p}/\mathfrak{p} \cong \mathbb{F}_q$. Sea $x \in U_{\mathfrak{p}}$, entonces se tiene

$$x = a_0 + a_1\pi + \cdots, \quad \text{con } a_0 \neq 0 \quad \text{y} \quad x^q \equiv a_0^q \pmod{\pi} \equiv a_0 \pmod{\pi} \equiv x \pmod{\pi},$$

es decir, $x^{N\mathfrak{p}-1} \equiv 1 \pmod{\pi}$.

En particular, si $x \in U_K \subseteq \mathcal{O}_{K_p}$, entonces $x^{N\mathfrak{p}-1} \in U_{1,\mathfrak{p}}$ y si $t := \prod_{\mathfrak{p}|p} (N\mathfrak{p} - 1) \in \mathbb{N}$, entonces $x^t \in E_1$, es decir, $U_K^t \subseteq E_1$. En particular, E_1 es de índice finito en U_K . Además, puesto que $U_K \cong \mathbb{Z}^{r_1+r_2-1} \times W(K)$ (Teorema de las Unidades de Dirichlet) como grupos, donde $W(K)$ denota a las raíces de unidad en K , se tiene que el rango sobre \mathbb{Z} de E_1 es $r_1 + r_2 - 1$.

Más precisamente, $E_1 \cong \mathbb{Z}^{r_1+r_2-1} \times (\text{finito})$ como grupos.

Por otro lado $U_{1,\mathfrak{p}}$ es un \mathbb{Z}_p -módulo con acción $s \circ u := u^s$ con $u \in U_{1,\mathfrak{p}}$, $s \in \mathbb{Z}_p$. Por lo anterior, $U_{1,\mathfrak{p}}$ es de índice finito en $U_{\mathfrak{p}}$ y por otro lado, para n suficientemente grande

$$U_{n,\mathfrak{p}} \cong U_{\mathfrak{p}}^{(n)} \xrightarrow[\log]{\exp} \mathfrak{p}^n \mathcal{O}_{K_p}.$$

Se sigue, como grupos, $U_{n,\mathfrak{p}} \cong \mathfrak{p}^n \cong \mathfrak{p} \cong \mathcal{O}_K$ ($\mathcal{O}_{K_p}/\mathfrak{p} \cong \mathbb{F}_q$ es el campo residual) y $\mathcal{O}_{K_p} \cong \mathbb{Z}_p^{[K_p:\mathbb{Q}_p]}$, $U_{n-1,\mathfrak{p}}/U_{n,\mathfrak{p}} \cong \mathbb{F}_q$.

De lo anterior obtenemos que

$$U_{1,\mathfrak{p}} \cong (\text{finito}) \times \mathfrak{p} \cong (\text{finito}) \times \mathbb{Z}_p^{[K_p:\mathbb{Q}_p]}.$$

En resumen tenemos

$$\begin{aligned} \mathbb{Z}^{r_1+r_2-1} \times (\text{finito}) \cong E_1 &\xrightarrow{\varphi} \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}} \cong (\text{finito}) \times \mathbb{Z}_p^{\sum [K_p:\mathbb{Q}_p]} \\ &\cong (\text{finito}) \times \mathbb{Z}_p^{[K:\mathbb{Q}]} \cong (\text{finito}) \times \mathbb{Z}_p^d \\ \varepsilon &\longmapsto (\varepsilon, \dots, \varepsilon) \end{aligned}$$

Usando la topología producto $\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$ se tiene que la cerradura \overline{E}_1 de E_1 (más precisamente, de $\varphi(E_1)$) en $\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$ es un \mathbb{Z}_p -módulo, es decir, $\overline{E}_1 \cong (\text{finito}) \times \mathbb{Z}_p^s$ para algún s , esto es, $\text{rango}_{\mathbb{Z}_p} \overline{E}_1 = s$. Puesto que $\text{rango}_{\mathbb{Z}} E_1 = r_1 + r_2 - 1$, se tiene $s \leq r_1 + r_2 - 1$.

Existe la siguiente conjetura:

Conjetura 13.5.9 (Leopoldt). Se tiene $\text{rango}_{\mathbb{Z}_p} \overline{E}_1 = s = r_1 + r_2 - 1$.

Observación 13.5.10. Se sabe que la conjetura de Leopoldt es cierta si la extensión K/\mathbb{Q} es abeliana.

Como consecuencia de la teoría de campos de clase, se tiene:

Teorema 13.5.11. Sea $0 \leq \delta \leq r_1 + r_2 - 1$ tal que $\text{rango}_{\mathbb{Z}_p} \overline{E}_1 = r_1 + r_2 - 1 - \delta$. Entonces hay exactamente $r_2 + 1 + \delta = d - \text{rango}_{\mathbb{Z}_p} \overline{E}$ ($d = [K : \mathbb{Q}]$) \mathbb{Z}_p -extensiones independientes de K . En otras palabras, si \tilde{K} denota la composición de todas las extensiones \mathbb{Z}_p de K , se tiene que $\text{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^{r_2+1+\delta}$, ($r_2 + 1 \leq r_2 + 1 + \delta \leq r_1 + 2r_2 = d$).

Antes de presentar un esquema de demostración de este resultado, recordemos un teorema de campos de clase. Sea k un campo numérico finito, $[k : \mathbb{Q}] < \infty$. Sea \mathfrak{p} un primo finito o infinito de k . Sea $k_{\mathfrak{p}}$ la completación de k en \mathfrak{p} , y $U_{\mathfrak{p}}$ las unidades locales de $k_{\mathfrak{p}}$. Si \mathfrak{p} es arquimideano, es decir infinito, ponemos $U_{\mathfrak{p}} = k_{\mathfrak{p}}^*$ ($= \mathbb{C}^*$ o \mathbb{R}^*). Se define el grupo de idèles de k por:

$$J_k := \left\{ (\dots, x_{\mathfrak{p}}, \dots) \in \prod_{\mathfrak{p}} k_{\mathfrak{p}}^* \mid x_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ para casi todo } \mathfrak{p} \right\}.$$

A J_k se le considera con la siguiente topología. Si $U = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$, a U se le dota de la topología producto y definimos a U como abierto en J_k . Más precisamente, J_k es un grupo topológico donde una base de vecindades de la unidad $1 = (\dots, 1, \dots)$ está dado por: para $S \subseteq \mathbb{P}_k = \{\mathfrak{p} \mid \mathfrak{p} \text{ es lugar de } k\}$, S finito y

$$\prod_{\mathfrak{p} \in S} V_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \subseteq J_k, \quad V_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^*$$

es una vecindad básica de $1 \in k_{\mathfrak{p}}^*$.

Se tiene que $\overline{V}_{\mathfrak{p}}$ es compacto y $\prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$ es compacto, por lo que cada vecindad de 1 en J_k contiene una vecindad

$$\prod_{\mathfrak{p} \in S} V_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$$

cuya cerradura es compacta. En otras palabras J_k , con la topología definida así, es un grupo topológico localmente compacto.

Sea

$$\begin{aligned} k^* &\xrightarrow{\theta} J_k \\ x &\longmapsto (\dots, x, \dots) = (x)_{\mathfrak{p} \in \mathbb{P}_K} \end{aligned}$$

Entonces θ es inyectiva, la imagen es un conjunto discreto. k^* , o más precisamente, $\theta(k^*)$ (Proposición 13.5.12) recibe el nombre de idèles principales.

Proposición 13.5.12. *Se tiene que k^* es discreto en J_k . En particular k^* es cerrado en J_k .*

Demostración. Es suficiente probar que $1 \in J_k$ tiene una vecindad que no contiene ningún otro idèle principal. Sea S el conjunto de primos arquimideanos y sea $V = \{\alpha \in J_k \mid |\alpha_{\mathfrak{p}} - 1| < 1 \text{ para } \mathfrak{p} \in S \text{ y } |\alpha_{\mathfrak{p}}| = 1, \text{ para } \mathfrak{p} \notin S\}$. Entonces si $B_{\mathfrak{p}}(1, 1)$ es la bola abierta de radio 1 y centro 1 en $k_{\mathfrak{p}}$, se tiene $V = \prod_{\mathfrak{p} \in S} B_{\mathfrak{p}}(1, 1) \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$.

Si hubiese un idèle principal $x \in V$ con $x \neq 1$, se tendría:

$$\begin{aligned} 1 &= \prod_{\mathfrak{p}} |x - 1|_{\mathfrak{p}} = \prod_{\mathfrak{p} \in S} |x - 1|_{\mathfrak{p}} \cdot \prod_{\mathfrak{p} \notin S} |x - 1|_{\mathfrak{p}} < \prod_{\mathfrak{p} \notin S} |x - 1|_{\mathfrak{p}} \\ &\leq \prod_{\mathfrak{p} \in S} \max\{|x|_{\mathfrak{p}}, 1\} = 1 \quad \text{pues } x \in k^*, x \in V. \end{aligned}$$

lo cual es absurdo. \square

Definición 13.5.13. Se define el grupo de clases de idèles por $C_k := J_k/k^*$.

Sea L/k una extensión finita. Si \mathfrak{P} es un primo de L y $\mathfrak{P}|_k = \mathfrak{p}$, sea $N_{\mathfrak{P}/\mathfrak{p}}: L_{\mathfrak{P}} \rightarrow k_{\mathfrak{p}}$ la norma de campos locales. Sea $x = (\dots, x_{\mathfrak{P}}, \dots) \in J_L$. Se define la norma de J_L a J_k por $N_{L/k}: J_L \rightarrow J_k$, $N_{L/k} = (\dots, y_{\mathfrak{p}}, \dots) \in J_k$ donde $y_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}/\mathfrak{p}} x_{\mathfrak{P}}$.

Si x es principal, esto es, $x = (\dots, x, \dots)$, entonces $y_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}/\mathfrak{p}} x_{\mathfrak{P}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}/\mathfrak{p}} x = N_{L/k} x$ para toda \mathfrak{p} y $N_{L/k}$ es la norma usual de L en k . Por tanto $N_{L/k}(x)$ es principal. Por tanto la norma $J_L \rightarrow J_k$ induce una norma de C_L en C_k : $N_{L/k}: C_L \rightarrow C_k$.

A continuación presentamos los teoremas fundamentales de la teoría de campos de clase sin demostración (ver Teoremas 11.8.2, 11.8.5 y Proposición 11.8.3).

Teorema 13.5.14. *Si L/k es una extensión abeliana finita, entonces existe un isomorfismo*

$$J_k/(k^* \cdot N_{L/k} J_L) \cong C_k/(N_{L/k} C_L) \cong \text{Gal}(L/k).$$

Además, el primo finito o infinito \mathfrak{p} es no ramificado en L/k si y sólo si $U_{\mathfrak{p}} \subseteq k^* N_{L/k} J_L$ donde $U_{\mathfrak{p}} \hookrightarrow J_k$ está dado por $u \mapsto (\dots, 1, \dots, 1, u, 1, \dots, 1, \dots)$. \square

Teorema 13.5.15. *Si H es un subgrupo abierto de C_k de índice finito, entonces existe una única extensión abeliana L/k tal que $N_{L/k} C_L = H$. Equivalentemente, si H es un abierto de índice finito en J_k y $k^* \subseteq H$, entonces existe una única extensión abeliana L/k tal que $k^* N_{L/k} J_L = H$. \square*

Teorema 13.5.16. *Si L_1 y L_2 son dos extensiones abelianas de k , entonces $L_1 \subseteq L_2 \iff k^*N_{L_1/k}J_{L_1} \supseteq k^*N_{L_2/k}J_{L_2}$.* \square

Los Teoremas 13.5.14, 13.5.15 y 13.5.16 se pueden enunciar para las extensiones infinitas de campos numéricos. Sea D_k la componente conexa de la identidad del grupo de clases de idèles C_k .

Teorema 13.5.17. (a) *Si L/k es una extensión abeliana entonces existe un subgrupo cerrado H de C_k con $D_k \subseteq H \subseteq C_k$ tal que $C_k/H \cong \text{Gal}(L/k)$. Además el primo \mathfrak{p} es no ramificado en $L/k \iff k^*U_{\mathfrak{p}}/k^* \subseteq H$.*
 (b) *Dado un subgrupo cerrado H de C_k tal que $D_k \subseteq H \subseteq C_k$ o, equivalentemente, C_k/H es totalmente desconexo, existe una única extensión abeliana L/k tal que $C_k/H \cong \text{Gal}(L/k)$.* \square

Ejemplo 13.5.18. Sea k un campo numérico y sea L el campo de clase de Hilbert de k , es decir, L es la máxima extensión abeliana no ramificada en todo primo finito o infinito. Puesto que L/k es no ramificada en todas partes, se tiene $U := \prod_{\mathfrak{p} \in \mathbb{P}_k} U_{\mathfrak{p}} \subseteq k^*N_{L/k}J_L$. Puesto que L/k es maximal con respecto a esta propiedad, k^*U es el grupo que corresponde a L de donde

$$J_k/k^*U \cong \text{Gal}(L/k).$$

Sea D_k el grupo de ideales de k y sea $\varphi: J_k \rightarrow D_k$ dada por: $\varphi((x)_{\mathfrak{p}}) = \prod_{\mathfrak{p} \text{ finito}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}$. Se tiene que φ está bien definida pues $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$ para casi toda \mathfrak{p} . Se tiene que $\text{nuc } \varphi = U$ y finalmente, ya que $\varphi^{-1}(\text{ideales principales}) = \varphi^{-1}(P_k)$ idèles principales, se sigue que $J_k/Uk^* \cong I_k/P_k = Cl_k =$ grupo de clases de k . En otras palabras

$$\text{Gal}(L/k) \cong Cl_k = \text{grupo de clases de ideales de } k.$$

Ahora regresamos al Teorema 13.5.11.

Teorema 13.5.11. *Si $[K : \mathbb{Q}] < \infty$ y \tilde{K} es la composición de todas las \mathbb{Z}_p -extensiones de K , entonces $\text{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^{r_2+1+\delta}$ donde $\text{rango}_{\mathbb{Z}_p} \bar{E}_1 = r_1 + r_2 - 1 - \delta$, $\delta \geq 0$.*

Demostración. Sea F la máxima extensión abeliana de K que es no ramificada fuera de p . Entonces $\tilde{K} \subseteq F$. Sea $J = K_K$. Del Teorema 13.5.17 obtenemos la existencia de un grupo cerrado H tal que $K^* \subseteq H \subseteq J$ tal que $J/H \cong \text{Gal}(F/K)$.

Sea $U_{\tilde{\ell}}$ el grupo de unidades locales de primo $\tilde{\ell}$ de K si $\tilde{\ell}$ es finito y ponemos $U_{\tilde{\ell}} = K_{\tilde{\ell}}^*$ si $\tilde{\ell}$ es arquimideano.

Sean $U' := \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$, $U'' := \prod_{\tilde{\ell}|p} U_{\tilde{\ell}}$ y $U := U' \times U''$. Poniendo 1 en el resto de las componentes, U' , U'' son subgrupos de J y U es abierto. Puesto que F/K es no ramificado fuera p , se tiene que $U'' \subseteq H$.

Puesto que F es maximal y H es cerrado, entonces $H = \overline{K^*U''}$. Sean $J' := J/H$ y $J'' := K^*U/H = K^*U'U''/H = U'H/H \cong U'/(U' \cap H)$. Ahora sea $U_1 := \prod_{\mathfrak{p}|p} U_{\mathfrak{p},1}$, donde $U_{\mathfrak{p},1}$ es el grupo de las unidades locales congruentes

con 1 módulo \mathfrak{p} . Como vimos anteriormente, se tiene que $U_{\mathfrak{p}}/U_{\mathfrak{p},1} \cong \mathbb{F}_q^*$, $\mathbb{F}_q = \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}$ es el campo residual. Por lo tanto U'/U_1 es finito. De hecho tenemos $U_{\mathfrak{p}} \cong \mu_{q-1} \times U_{\mathfrak{p},1}$ pues $U_{\mathfrak{p},1}$ contiene a lo más p^s raíces de 1, $q = p^n$, $p = \text{car } \mathbb{F}_q$. Por lo tanto $U' = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}} \cong (\text{finito}) \times \prod_{\mathfrak{p}|p} U_{\mathfrak{p},1} = (\text{finito}) \times U_1 = T \times U_1$ con T

finito y de orden primo relativo a p . Así $U_1 \cong (p\text{-grupo finito}) \times \mathbb{Z}_p^{[K:\mathbb{Q}]}$. Por otro lado si $U_{\mathfrak{p},n} := \{x \in U_{\mathfrak{p}} \mid x \equiv 1 \text{ mód } \mathfrak{p}^n\}$, se tiene $U_{\mathfrak{p},n}/U_{\mathfrak{p},n+1} \cong \mathbb{F}_q$.

Por lo tanto $|U_{\mathfrak{p},1}/U_{\mathfrak{p},n}| = q^{n-1}$ y para n suficientemente grande, $U_{\mathfrak{p},n} \cong \mathfrak{p}^n \cong \mathcal{O}_{K_{\mathfrak{p}}} \cong \mathbb{Z}_p^{[K_{\mathfrak{p}}:\mathbb{Q}]}$. Se sigue que $U' = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}} = T \times \prod_{\mathfrak{p}|p} U_{\mathfrak{p},1} = T \times U_1$, $\text{mcd}(|T|, p) = 1$. Así se tiene que si $C = J'' = U'/(U' \cap H)$ entonces $C = (\text{finito}) \times \frac{U_1(U' \cap H)}{U' \cap H}$ pues $U' \cong T \times U_1$.

Si definimos $A_1 := TM/M$ donde $M := U \cap H$ y $B_1 := U_1M/M$, entonces $A_1, B_1 \subseteq C$ y puesto que $U' = TU_1$, se sigue que $A_1 + B_1 = C$. Por otro lado A_1 es un cociente de T y por tanto finito y de orden primo relativo a p y B es un cociente de U_1 de donde tenemos $B_1 \cong (p\text{-grupo finito}) \times \mathbb{Z}_p^\beta$.

En particular, $A_1 \cap B_1 = \{0\}$ por lo que $C \cong A_1 \oplus B_1$ y por tanto $C \cong (\text{finito}) \times U_1M/M$. Así, tenemos

$$J'' = (\text{finito}) \times \frac{U_1(U' \cap H)}{U' \cap H} \cong (\text{finito}) \times \frac{U_1}{U_1 \cap U \cap H} = (\text{finito}) \times \frac{U_1}{U_1 \cap H}.$$

Sea $\psi: E_1 \rightarrow U_1 \subseteq J$ el mapeo diagonal en U_1 y con 1 en las otras entradas, es decir,

$$\psi(\varepsilon) = (\dots, 1, \dots, \varepsilon, \dots, \dots) \quad \text{con } \varepsilon \text{ si } \mathfrak{p}|p \text{ y } 1 \text{ si } \mathfrak{p} \nmid p.$$

$$\text{En otras palabras } \psi(\varepsilon) = (x_{\mathfrak{p}})_{\mathfrak{p}}, \quad x_{\mathfrak{p}} = \begin{cases} \varepsilon & \text{si } \mathfrak{p}|p \\ 1 & \text{si } \mathfrak{p} \nmid p \end{cases}.$$

Antes de continuar con la demostración, probemos:

Lema 13.5.19. *Se tiene $U_1 \cap H = U_1 \cap \overline{K^*U''} = \overline{\psi(E_1)}$.*

Demostración (Lema 13.5.19). Sea $\varepsilon \in E_1$, $\psi(\varepsilon) \in U_1$ y puesto que $\frac{\psi(\varepsilon)}{\varepsilon}$ tiene componente 1 en todas las entradas tales que $\mathfrak{p} \nmid p$, se tiene $\psi(\varepsilon) = \varepsilon \cdot \frac{\psi(\varepsilon)}{\varepsilon} \in K^*U''$. Por tanto $\overline{\psi(E_1)} \subseteq U_1 \cap \overline{K^*U''}$.

Recíprocamente, sea $U_{\mathfrak{p},n} = 1 + \mathfrak{p}^n = \{x \in U_{\mathfrak{p}} \mid x \equiv 1 \text{ mód } \mathfrak{p}^n\}$ y sea $U_n := \prod_{\mathfrak{p}|p} U_{\mathfrak{p},n}$. Poniendo 1 en todas las componentes tales que $\mathfrak{p} \nmid p$ se tiene que

$$K^*U''U_n = \bigcup_{x \in K^*} (x \cdot U'' \cdot U_n)$$

es abierto y $\overline{K^*U''} = \bigcap_{n=1}^{\infty} K^*U''U_n$ pues si $x \in K^*U''$, entonces $x(U'' \times U_n) \cap K^*U'' \neq \emptyset$, $xy = \xi t$ para $y \in U'' \times U_n$, $\xi \in K^*$, $t \in U''$ por lo que $x = y^{-1}\xi t = \xi ty^{-1} \in K^*U''U_n$ de donde $\overline{K^*U''} \subseteq \bigcap_{n=1}^{\infty} K^*U''U_n$ y recíprocamente si $x \notin \overline{K^*U''}$ existe una vecindad V de 1 tal que $xV \cap K^*U'' = \emptyset$. Entonces existe $n \geq 1$ tal que $V \supseteq U_n \times \prod_{\mathfrak{p} \in S} W_{\mathfrak{p}} \times \prod_{\substack{\mathfrak{p} \notin S \\ \mathfrak{p} \nmid p}} U_{\mathfrak{p}}$ donde S es un conjunto finito

de lugares \mathfrak{p} donde $\mathfrak{p} \nmid p$.

Si $x \in K^*U''U_n$, $x = \xi ty$ con $\xi \in K^*$, $t \in U''$, $y \in U_n$. Por tanto $xy^{-1} = \xi t \in xV \cap K^*U''$ lo cual es absurdo. Así pues, $x \notin K^*U''U_n$ y por tanto $\overline{K^*U''} \supseteq \bigcap_{n=1}^{\infty} K^*U''U_n$ de donde obtenemos la igualdad anunciada: $\overline{K^*U''} = \bigcap_{n=1}^{\infty} K^*U''U_n$.

Similarmente tenemos $\overline{\psi(E_1)} = \bigcap_{n=1}^{\infty} \psi(E_1)U_n$, y U_n es compacto. Para verificar que $U_1 \cap \overline{K^*U''} \subseteq \overline{\psi(E_1)}$, basta probar que $U_1 \cap K^*U''U_n \subseteq \psi(E_1)U_n$ para toda n .

Sea $x \in K^*$, $u'' \in U''$, $x \in U_n \subseteq U_1$, $xu''u \in U_1$ por lo que $xu'' \in U$. Ahora bien, u'' tiene componente 1 en todas las entradas tales que $\mathfrak{p} \nmid p$ y x debe ser una unidad principal en las componentes $\mathfrak{p}|p$.

Ahora U_1 tiene componentes 1 para $\mathfrak{p} \nmid p$ y u'' es una unidad ahí, por lo que x debe ser una unidad en esas entradas. En resumen, x es unidad local para toda \mathfrak{p} por lo que x debe ser una unidad global además de que $x \equiv 1 \pmod{\mathfrak{p}}$ lo cual implica que $x \in E_1$.

Así tenemos $xu'' = x \in E_1$ para $\mathfrak{p}|p$. Para $\mathfrak{p} \nmid p$, $xu'' = 1$ por tanto $xu'' \in \psi(E_1)$ y por lo tanto $xu''u \in \psi(E_1)U_n$. Esto termina la demostración del lema. \square

Regresando a la demostración del Teorema 13.5.11, recordemos que $U_1 \cong (\text{finito}) \times \mathbb{Z}_p^{[K:\mathbb{Q}]}$ por lo que $U_1/(U_1 \cap H) = U_1/(\overline{\psi(E_1)}) \cong (\text{finito}) \times \mathbb{Z}_p^{\alpha}$ donde

$$\alpha = [K:\mathbb{Q}] - \text{rango}_{\mathbb{Z}_p} \overline{\psi(E_1)} = r_1 + 2r_2 - (r_1 + r_2 - 1 - \delta) = r_2 + 1 + \delta.$$

Por tanto $J'' \cong (\text{finito}) \times \frac{U_1}{(U_1 \cap H)} \cong (\text{finito}) \times \mathbb{Z}_p^{r_2+1+\delta}$, $(J'' \cong \frac{K^*U}{H})$.

Teníamos que $J' = J/H$, $H = \overline{K^*U''}$. Ahora

$$J'/J'' \cong J/K^*U = Cl_K$$

donde Cl_K es el grupo de clases de ideales de K el cual es finito. Además, $J'/\mathbb{Z}_p^{r_2+1+\delta} \cong (\text{finito}) = T_1$, digamos $|T_1| = m$.

Se tiene que $m\mathbb{Z}_p^{r_2+1+\delta} \subseteq mJ' \subseteq \mathbb{Z}_p^{r_2+1+\delta}$ por lo que $mJ' \cong \mathbb{Z}_p^{r_2+1+\delta}$ como \mathbb{Z}_p -módulos.

Sea $J'_m = \{x \in J' \mid mx = 0\}$. Entonces J'_m es cerrado en J' y $J'/J'_m \cong mJ' \cong \mathbb{Z}_p^{r_2+1+\delta}$.

Ahora bien $|J'_m| \leq m$ pues en caso contrario, esto es, si $|J'_m| > m$, y puesto que $J'/\mathbb{Z}_p^{r_2+1+\delta} \cong T_1$, entonces tendríamos dos elementos $x, y \in J'_m$, $x \neq y$, $x \bmod \mathbb{Z}_p^{r_2+1+\delta} = y \bmod \mathbb{Z}_p^{r_2+1+\delta}$ y $m(x - y) = 0$ lo cual no es posible pues $x - y \in \mathbb{Z}_p^{r_2+1+\delta}$ es no cero y $\mathbb{Z}_p^{r_2+1+\delta}$ es libre de torsión.

Así, $|J'_m| \leq m < \infty$. Finalmente el campo fijo de $J'_m \subseteq J' \cong \text{Gal}(F/K)$ debe ser K y por lo tanto

$$\text{Gal}(\tilde{K}/K) \cong J'/J'_m \cong \mathbb{Z}_p^{r_2+1+\delta}. \quad \square$$

Corolario 13.5.20. *Sea K_H el campo de clase de Hilbert de un campo numérico finito K y sea F la máxima extensión abeliana de K no ramificada fuera de p . Entonces*

$$\text{Gal}(F/K_H) \cong \frac{\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}}{\overline{E}}$$

donde \overline{E} es la cerradura del grupo de unidades E de K cuando en encajado diagonalmente en $\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$ y $U_{\mathfrak{p}}$ es el grupo de unidades locales de $K_{\mathfrak{p}}$.

Demostración. Se tiene que $\text{Gal}(F/K) \cong J' = J/H$ y el subgrupo cerrado $J'' = KU/H$ corresponde a K_H . Por lo tanto $\text{Gal}(F/K_H) \cong J'' \cong U'/(U' \cap H)$. Como antes, se tiene que $U' \cap H = \overline{\psi(E)}$ y el resultado se sigue. \square

Corolario 13.5.21. \mathbb{Q} sólo tiene una extensión \mathbb{Z}_p .

Demostración. $[\mathbb{Q} : \mathbb{Q}] = 1 = r_1 + 2r_2$, $r_1 = 1$, $r_2 = 0$, $0 \leq \text{rango}_{\mathbb{Z}_p} \overline{E}_1 = r_1 + r_2 - 1 - \delta \leq r_1 + r_2 - 1 = 1 + 0 - 1 = 0$. Por lo tanto $\delta = 0$ y $r_2 + 1 + \delta = 0 + 1 + 0 = 1$.

De hecho, $E_1 = \{x \in U_{\mathbb{Q}} \mid x \equiv 1 \bmod p\} = \{1\}$, por lo que $\overline{E}_1 = \{1\}$ y por lo tanto $\text{rango}_{\mathbb{Z}_p} E_1 = 0$.

Una tercera demostración es simplemente que

$$1 = 0 + 1 = r_2 + 1 \leq \text{número de extensiones } \mathbb{Z}_p \text{ de } \mathbb{Q} \leq d = [\mathbb{Q} : \mathbb{Q}] = 1. \quad \square$$

Observación 13.5.22. Se tiene que $\mathbb{Z}_p \times \mathbb{Z}_p$ no puede ser el grupo de Galois de ninguna extensión K/\mathbb{Q} .

El problema inverso de la Teoría de Galois pregunta si dado G un grupo finito, existe una extensión de Galois K de \mathbb{Q} tal que $\text{Gal}(K/\mathbb{Q}) \cong G$. Ya vimos que si G es abeliano la respuesta es si (Teorema 6.4.13; ver también Teorema 6.4.14).

Sin embargo, si G es infinito vemos que la respuesta al problema inverso a la Teoría de Galois es en general no, aunque el grupo G sea abeliano, por ejemplo $G = \mathbb{Z}_p \times \mathbb{Z}_p$.

13.6. Estructura de $\Lambda = \mathbb{Z}_p[[T]]$ -módulos

En esta sección consideraremos una \mathbb{Z}_p -extensión K_∞/K y ponemos $\text{Gal}(K_\infty/K) \cong \Gamma = \mathbb{Z}_p$, Γ escrito multiplicativamente.

Por un lado tenemos que varios módulos relacionados con la extensión K_∞/K tienen una acción dada por Γ , considerado Γ como el grupo de Galois y, por otro lado, tienen una acción del grupo aditivo \mathbb{Z}_p , no considerado como grupo de Galois. Juntando ambas acciones tendremos varios $\mathbb{Z}_p[\Gamma]$ -módulos. Esta es la razón de denotar $\text{Gal}(K_\infty/K)$ por Γ en lugar de \mathbb{Z}_p .

Sea γ un generador topológico de Γ , es decir, $\overline{\langle \gamma \rangle} = \Gamma$. Por ejemplo, bajo el isomorfismo $\Gamma \xrightarrow{\cong} \mathbb{Z}_p$, γ puede corresponder a $1 \in \mathbb{Z}_p$.

Se tiene que $\Gamma^{p^n} \cong p^n \mathbb{Z}_p$. Sea $\Gamma_n := \Gamma / \Gamma^{p^n} \cong C_{p^n}$, el grupo cíclico de p^n elementos. Entonces $\Gamma_n \cong \text{Gal}(K_n/K) = \langle \gamma \text{ mód } \Gamma^{p^n} \rangle$.

Sea \mathcal{O} el anillo de enteros de una extensión finita de \mathbb{Q}_p y sea \mathfrak{p} el ideal maximal de \mathcal{O} y π un elemento primo de \mathfrak{p} , es decir, $\mathfrak{p} = \langle \pi \rangle$.

Consideremos el anillo grupo $\mathcal{O}[\Gamma_n]$. Si $m \geq n \geq 0$, sea $\phi_{m,n}: \mathcal{O}[\Gamma_m] \rightarrow \mathcal{O}[\Gamma_n]$ el mapeo inducido por el mapeo natural $\psi_{m,n}: \Gamma_m \rightarrow \Gamma_n$.

Se tiene que $\mathcal{O}[\Gamma_n] \cong \frac{\mathcal{O}[T]}{(1+T)^{p^n}-1}$ con isomorfismo

$$\gamma \text{ mód } \Gamma^{p^n} \xrightarrow{\xi} (1+T) \text{ mód } ((1+T)^{p^n} - 1).$$

Se tiene el siguiente diagrama conmutativo para $m \geq n \geq 0$:

$$\begin{array}{ccc} \mathcal{O}[\Gamma_m] & \xrightarrow{\xi} & \mathcal{O}[T]/((1+T)^{p^m}-1) \\ \downarrow \phi_{m,n} & & \downarrow \phi'_{m,n} \\ \mathcal{O}[\Gamma_n] & \xrightarrow{\xi} & \mathcal{O}[T]/((1+T)^{p^n}-1) \end{array}$$

donde $\phi'_{m,n}$ es el mapeo natural pues $((1+T)^{p^n}-1) | ((1+T)^{p^m}-1)$.

Sea $\varprojlim_n \mathcal{O}[\Gamma_n] \cong \mathcal{O}[[\Gamma]]$ el anillo de grupo profinito. En general se tiene que $\mathcal{O}[\Gamma] \subseteq \mathcal{O}[[\Gamma]]$ pues si $\alpha \in \mathcal{O}[\Gamma]$, entonces $\alpha = \sum_{\sigma \in \Gamma} a_\sigma \sigma$ con $a_\sigma = 0$ para casi toda $\sigma \in \Gamma$. Sea $\alpha_n := \sum_{\sigma \in \Gamma_n} a_\sigma \phi_n(\sigma)$ donde $\phi_n: \Gamma \rightarrow \Gamma_n$ es el mapeo asociado con $\varprojlim_n \Gamma_n = \Gamma$. Entonces $\alpha \in \mathcal{O}[\Gamma_n]$ y claramente $\phi_{m,n}(\alpha_m) = \alpha_n$.

Sin embargo $\mathcal{O}[\Gamma] \subsetneq \mathcal{O}[[\Gamma]]$ como veremos más adelante.

Se tiene

$$\mathcal{O}[[\Gamma]] = \varprojlim_n \mathcal{O}[\Gamma_n] \cong \varprojlim_n \mathcal{O}[T]/((1+T)^{p^n}-1).$$

Veremos que $\mathcal{O}[[\Gamma]] \cong \mathcal{O}[[T]]$.

Proposición 13.6.1 (Algoritmo euclideo). Sean $f, g \in \mathcal{O}[[T]]$ y $f = a_0 + a_1T + \cdots$ con $a_i \in \mathfrak{p}$, $0 \leq i \leq n-1$ y $a_n \in \mathcal{O}^*$. Entonces se tiene una única expresión del tipo $g = qf + r$ con $q \in \mathcal{O}[[T]]$, $r \in \mathcal{O}[T]$, r un polinomio de grado menor o igual a $n-1$.

Demostración. Primero probaremos la unicidad de la expresión. Basta probar que si $qf + r = 0$ entonces $q = r = 0$. Supongamos que q o r no es cero. Podemos suponer que $\pi \nmid r$ o $\pi \nmid q$. Puesto que el grado de r es menor o igual a $n-1$ y $\pi|a_i$, $0 \leq i \leq n-1$, tomando módulo π , se tiene que $\pi|r$ y por tanto $\pi|qf$. Puesto que $a_n \in \mathcal{O}^*$, $\pi \nmid f$ de donde se sigue que $\pi|q$ lo cual contradice nuestra elección. Por lo tanto $q = r = 0$ lo cual prueba la unicidad.

Para demostrar la existencia, sea $\tau = \tau_n: \mathcal{O}[[T]] \rightarrow \mathcal{O}[[T]]$ dado por $\tau\left(\sum_{i=0}^{\infty} b_i T^i\right) = \sum_{i=n}^{\infty} b_i T^{i-n} = b_n + b_{n+1}T + \cdots$.

Se tiene que τ es \mathcal{O} -lineal y satisface:

- (a) $\tau(T^n h(T)) = h(T)$ para toda $h(T) \in \mathcal{O}[[T]]$.
- (b) $\tau(h(T)) = 0 \iff h(T) \in \mathcal{O}[T]$, con $\text{gr } h(T) \leq n-1$.

Por hipótesis podemos escribir

$$f(T) = \pi P(T) + T^n U(T)$$

con $P(T) \in \mathcal{O}[T]$, $\text{gr } P \leq n-1$ y $U(T) = a_n + a_{n+1}T + \cdots = \tau(f(T)) \in \mathcal{O}[[T]]$.

Para tener $g = qf + r$, $\text{gr } r \leq n-1$ es necesario y suficiente que $\tau(g) = \tau(qf)$. Puesto que $qf = \pi Pq + T^n qU$ necesitamos resolver

$$\tau(g) = \tau(\pi qf) + \tau(T^n qU) = \tau(\pi qP) + qU = \tau(\pi qP) + q\tau(f).$$

Ahora bien, $\tau(f) = U$ es invertible. Sea $z = qU = q\tau(f)$. La ecuación anterior equivale a

$$\tau(g) = \tau\left(\frac{\pi q}{U}PU\right) + z = \tau\left(z \cdot \frac{\pi P}{\tau(f)}\right) + z = \left(I + \tau \cdot \frac{\pi P}{\tau(f)}\right)(z).$$

Notemos que $\tau \cdot \frac{\pi P}{\tau(f)}: \mathcal{O}[[T]] \rightarrow \mathfrak{p}\mathcal{O}[[T]]$ pues $\frac{\pi P}{\tau(f)} \in \mathfrak{p}\mathcal{O}[[T]]$ por lo tanto se puede invertir $(I + \tau \cdot \frac{\pi P}{\tau(f)})$:

$$\begin{aligned} Uq = z &= \left(I + \tau \cdot \frac{\pi P}{\tau(f)}\right)^{-1} \tau(g) = \sum_{j=0}^{\infty} \left(\tau \cdot \frac{\pi P}{\tau(f)}\right)^j \tau(g) \\ &= \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \cdot \frac{P}{U}\right)^j \cdot \tau(g), \end{aligned}$$

por lo tanto

$$q = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \cdot \frac{P}{U}\right)^j \cdot \tau(g). \quad \square$$

Definición 13.6.2. Un polinomio $p(T) \in \mathcal{O}[T]$ se llama *distinguido* si $p(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$ con $a_i \in \mathfrak{p}$ para $0 \leq i < n-1$. Notemos que $p(T)$ “casi” es de Eisenstein con la salvedad de que posiblemente $\pi^2 | a_0$.

Teorema 13.6.3 (Teorema p -ádico de Preparación de Weierstrass). Sea $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[[T]]$ tal que para alguna $n \geq 0$, se tiene que $a_i \in \mathfrak{p}$, $0 \leq i \leq n-1$ pero $a_n \notin \mathfrak{p}$, esto es, $a_n \in \mathcal{O}^*$. Entonces f puede ser escrito de manera única en la forma

$$f(T) = p(T)U(T)$$

con $U(T) \in \mathcal{O}[[T]]$ es unidad y $p(T)$ es un polinomio distinguido de grado n .

Más generalmente, si $f(T) \in \mathcal{O}[[T]] \setminus \{0\}$, f puede ser escrito de manera única como $f(T) = \pi^u P(T)U(T)$ como antes y $u \geq 0$.

Demostración (Manin). Notemos que la segunda parte es inmediata de la primera donde π^u es la máxima potencia de π que divide a todos los coeficientes de f .

Sea $g = T^n$. Entonces, por el algoritmo euclideo, se tiene que $T^n = q(T)f(T) + r(T)$, gr $r \leq n-1$.

Puesto que $q(T)f(T) \equiv q(T)(a_n T^n + T^{n+1}h(T)) \pmod{\pi}$ por lo que $r(T) \equiv 0 \pmod{\pi}$. Por lo tanto $p(T) = T^n - r(T)$ es un polinomio distinguido de grado n . Sea $q_0 := q(0)$. Comparando coeficientes de T^n , se tiene que $1 = q_0 a_n \pmod{\pi}$ lo cual implica que $q_0 \in \mathcal{O}^*$ así que $q(T)$ es una unidad.

Sea $U(T) = \frac{1}{q(T)}$ lo que nos da $f(T) = P(T)U(T)$.

Para la unicidad, puesto que todo polinomio distinguido de grado n puede ser escrito como $p(T) = T^n - r(T)$, la ecuación $f(T) = P(T)U(T)$ puede ser escrito de nuevo como $T^n = U(T)^{-1}f(T) + r(T)$ y por la unicidad del algoritmo euclideo, se sigue la unicidad de $f(T) = P(T)U(T)$. \square

Corolario 13.6.4. Sea $\overline{\mathbb{Q}}_p$ una cerradura algebraica de \mathbb{Q}_p y sea \mathbb{C}_p la completación de $\overline{\mathbb{Q}}_p$. Se tiene que como campos, $\mathbb{C} \cong \mathbb{C}_p$ más no topológicamente. En particular \mathbb{C}_p es algebraicamente cerrado. Entonces, existen un número finito de elementos $x \in \mathbb{C}_p$ tales que $|x| < 1$ y $f(x) = 0$.

Demostración. Sea $f(x) = 0$ y escribamos $f(T) = \pi^u P(T)U(T)$ como en el Teorema de Preparación de Weierstrass. Puesto que $U(x) \neq 0$, es invertible, $U(x)$ converge para $|x| < 1$. Por lo tanto $P(x) = 0$. De ahí se sigue el resultado. \square

Lema 13.6.5. Supongamos $P(T) \in \mathcal{O}[T]$ un polinomio distinguido y sea $g(T) \in \mathcal{O}[T]$ arbitrario. Si $g(T)/P(T) \in \mathcal{O}[[T]]$, entonces $g(T)/p(T) \in \mathcal{O}[T]$.

Demostración. Supongamos $g(T) = f(T)P(T)$ con $f(T) \in \mathcal{O}[[T]]$. Sea $x \in \mathbb{C}_p$ un cero de $P(T)$. Por tanto $0 = P(x) = x^n + \pi\alpha$ lo cual implica que $|x| < 1$ y por lo tanto $f(x)$ converge. Se sigue que $g(x) = 0$. Dividiendo entre $T - x$ y ampliando el anillo \mathcal{O} en caso necesario, obtenemos que $P(T)|g(T)$ como polinomios, por lo tanto en $\mathcal{O}[T]$. \square

Teorema 13.6.6 (J.-P. Serre). *Se tiene $\mathcal{O}[[T]] \cong \mathcal{O}[[T]]$ el isomorfismo inducido por $\gamma: \mapsto 1+T$.*

Demostración. Es suficiente probar que $\mathcal{O}[[T]] \cong \varprojlim_n \frac{\mathcal{O}[T]}{\langle (1+T)^{p^n} - 1 \rangle}$.

Notemos que $p_n(T) = (1+T)^{p^n} - 1$ es un polinomio distinguido. De hecho, $\langle \pi, T \rangle \supseteq \langle p, T \rangle$ es un ideal maximal de $\mathcal{O}[T]$ y también da el ideal maximal de $\mathcal{O}[[T]]$. Ahora $P_0(T) = (1+T)^{p^0} - 1 = T \in \langle p, T \rangle$. Además

$$\begin{aligned} \frac{P_{n+1}(T)}{P_n(T)} &= \frac{(1+T)^{p^{n+1}} - 1}{(1+T)^{p^n} - 1} = \frac{y^p - 1}{y - 1} = y^{p-1} + y^{p-2} + \cdots + y + 1 \\ &\quad \uparrow \\ &\quad y = (1+T)^{p^n} \\ &= (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + \cdots + (1+T)^{p^n} + 1 \in \langle p, T \rangle. \end{aligned}$$

Por inducción en n se sigue que $P_n(T) \in \langle p, T \rangle^{n+1}$. Por el algoritmo euclidiano, para cada $f(T) \in \mathcal{O}[[T]]$, $f(T) = q_n(T)P_n(T) + f_n(T)$, gr $f_n(T) < p^n$. Entonces $f(T) \rightarrow f_n(T)$ es un mapeo natural: $\mathcal{O}[[T]] \rightarrow \frac{\mathcal{O}[T]}{\langle P_n(T) \rangle}$ y si $m \geq n \geq 0$ entonces

$$f_m(T) - f_n(T) = p_n(T) \left(q_n(T) - q_m(T) \frac{P_m(T)}{P_n(T)} \right).$$

Por lo tanto $P_n(T) | f_m(T) - f_n(T)$ como polinomios (Lema 13.6.5).

Por lo tanto $f_m(T) \equiv f_n(T) \pmod{P_n(T)}$. Se sigue que $(f_0, f_1, \dots) \in \varprojlim_n \frac{\mathcal{O}[T]}{\langle P_n(T) \rangle}$. Así tenemos un mapeo:

$$\begin{aligned} \mathcal{O}[[T]] &\xrightarrow{\varphi} \varprojlim_n \frac{\mathcal{O}[T]}{\langle P_n(T) \rangle} \\ f &\mapsto (f_0, f_1, \dots) \end{aligned}$$

Ahora si $f_n = 0$ para toda n , $P_n | f$ para toda n . Por tanto $f \in \bigcap_{n=0}^{\infty} \langle p, T \rangle^{n+1} = (0)$ de donde se sigue que φ es 1-1.

Sea ahora $(f_0, f_1, \dots) \in \varprojlim_n \frac{\mathcal{O}[T]}{\langle P_n(T) \rangle}$. Por lo tanto, para $m \geq n \geq 0$, $f_m \equiv f_n \pmod{P_n}$, es decir, $f_m \equiv f_n \pmod{\langle p, T \rangle^{n+1}}$. Se sigue que los términos constantes son congruentes módulo p^{n+1} , los términos lineales son congruentes módulo p^n , etc.

Así, los coeficientes f_m forman una sucesión de Cauchy. Alternativamente $f = \lim_{n \rightarrow \infty} f_n$ existe pues $\mathcal{O}[[T]]$ es completo en la topología $\langle p, T \rangle$ -ádica. Sea $f(T) := \lim_{n \rightarrow \infty} f_n(T) \in \mathcal{O}[[T]]$. Veremos que $\varphi(f) = (f_0, f_1, \dots)$.

Si $m \geq n \geq 0$, $f_m - f_n = q_{m,n}P_n$ para algún $q_{m,n} \in \mathcal{O}[T]$. Entonces $q_{m,n} = \frac{f_m - f_n}{P_n} \xrightarrow{m \rightarrow \infty} \frac{f - f_n}{P_n}$. Puesto que $q_{m,n} \in \mathcal{O}[T]$, el límite debe estar en $\mathcal{O}[[T]]$, es decir, sin denominadores. Por lo tanto $f = (P_n) \left(\lim_{m \rightarrow \infty} q_{m,n} \right) + f_n$, esto es, $\varphi(f) = (f_0, f_1, \dots)$ y φ es suprayectiva. \square

Lema 13.6.7. *Se tiene que $\Lambda = \mathbb{Z}_p[[T]]$ es un dominio de factorización única cuyos irreducibles son p y los polinomios distinguidos irreducibles.*

Las unidades de Λ^ de Λ son las series de potencias con termino constante en \mathbb{Z}_p^* .*

Demostración. Dado $f(T) \in \mathbb{Z}_p[[T]]$, se tiene que por el Teorema de Preparación de Weierstrass, $f(T)$ se puede escribir de manera única como $f(T) = p^u P(T)U(T)$ con $u \in \mathbb{Z}$, $u \geq 0$, $p(T)$ un polinomio distinguido y $U(T) \in \Lambda^*$. Por el Lema 13.6.5 se tiene que si $f(T) \in \mathbb{Z}_p[T]$, entonces $U(T) \in \mathbb{Z}_p[T]$.

Ahora, en $\mathbb{Z}_p[T]$, $P(T)$ es producto único de polinomios mónicos e irreducibles: $P(T) = P_1(T) \cdots P_r(T)$. Ahora $P(T) \bmod p = T^n$. Por lo tanto $P_i(T) \bmod p = T^{n_i}$, $1 \leq i \leq r$, $n = n_1 + \cdots + n_r$ y cada $P_i(T)$ es un polinomio distinguido. Por lo tanto $\mathbb{Z}_p[[T]]$ es un dominio de factorización única (D.F.U.) y sus irreducibles son p y los polinomios distinguidos irreducibles. \square

Observación 13.6.8. Se tiene que $\Lambda = \mathbb{Z}_p[[T]]$ no es un dominio de ideales principales. En particular no tenemos los teoremas estructurales de los dominios de ideales principales en esta clase de dominios. Sin embargo, $\Lambda = \mathbb{Z}_p[[T]]$ es dominio de factorización única y noetheriano pues \mathbb{Z}_p es noetheriano.

Lema 13.6.9. *Sean $f, g \in \Lambda$ primos relativos. Entonces el anillo $\Lambda/\langle f, g \rangle$ es finito.*

Demostración. Sea $h \in \langle f, g \rangle$ un elemento de grado mínimo. Entonces $h = p^s H$ con $H = 1$ o H distinguido. Supongamos que $H \neq 1$. Puesto que f y g son primos relativos, podemos suponer que $H \nmid f$. Sin embargo

$$f = qH + r, \quad \text{gr } r < \text{gr } H = \text{gr } h \quad \text{por lo que} \quad p^s f = qh + p^s r$$

y puesto $\text{gr}(p^s r) = \text{gr } r < \text{gr } h$, $p^s r \in \langle f, g \rangle$ y $p^s r \neq 0$ pues $H \nmid f$, esto es absurdo. Por lo tanto $H = 1$ y $h = p^s$. Sin pérdida de generalidad, podemos suponer que $p \nmid f$ y que f es distinguido pues en otro caso se puede usar g o dividir por una unidad ya que f y g son primos relativos. Se tiene que $\langle f, g \rangle \supseteq \langle p^s, f \rangle$.

Por el algoritmo euclideo, dado $\alpha(T) \in \Lambda$, $\alpha \bmod f \equiv r$ con $\text{gr } r < \text{gr } f$ y puesto que sólo hay un número finito de tales polinomios módulo p^s , entonces

$$|\Lambda/\langle p^s, f \rangle| < \infty \quad \text{y} \quad |\Lambda/\langle f, g \rangle| \leq |\Lambda/\langle p^s, f \rangle| < \infty. \quad \square$$

Lema 13.6.10 (Casi “Teorema Chino del Residuo”). *Sean $f, g \in \Lambda$ primos relativos. Entonces*

(I) *el mapeo natural*

$$\begin{aligned} \Lambda/\langle f, g \rangle &\xrightarrow{\tilde{\varphi}} \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle \\ h \bmod \langle f, g \rangle &\mapsto (h \bmod \langle f \rangle, h \bmod \langle g \rangle) \end{aligned}$$

es inyectivo y tiene conúcleo finito.

(II) Existe un mapeo inyectivo $\Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle \xrightarrow{\psi} \Lambda/\langle f, g \rangle$ que tiene conúcleo finito.

Demostración. (I) Por ser Λ un dominio de factorización única, si $h \in \text{núc } \varphi$, donde $\varphi: \Lambda \rightarrow \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle$, se tiene que $h \text{ mód } \langle f \rangle = 0$ y $h \text{ mód } \langle g \rangle = 0$, de donde obtenemos que $f|h$ y $g|h$ y por lo tanto $fg|h$ lo cual implica que $\tilde{\varphi}: \Lambda/\langle f, g \rangle \rightarrow \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle$ es inyectivo.

Sea ahora $(a \text{ mód } \langle f \rangle, b \text{ mód } \langle g \rangle) \in \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle$. Si $a - b \in \langle f, g \rangle$ entonces $a - b = fA + gB$ para algunos $A, B \in \Lambda$. Sea $c := a - fA = b + gB$. Entonces $c \equiv a \text{ mód } \langle f \rangle$ y $c \equiv b \text{ mód } \langle g \rangle$ y en este caso $(a \text{ mód } \langle f \rangle, b \text{ mód } \langle g \rangle)$ está en la imagen de $\tilde{\varphi}$.

Puesto que $|\Lambda/\langle f, g \rangle| = n < \infty$, podemos seleccionar $r_1, \dots, r_n \in \Lambda$ un conjunto de representantes de $\Lambda/\langle f, g \rangle$. En particular, tendremos que $\{(0 \text{ mód } \langle f \rangle, r_j \text{ mód } \langle g \rangle) \mid 1 \leq j \leq n\}$ es un conjunto de representantes del conúcleo de $\tilde{\varphi}$ (ejercicio) y por lo tanto el conúcleo es finito.

(II) Sea $\Lambda/\langle f, g \rangle \cong M \subseteq \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle =: N$. Se tiene que $|N/M| < \infty$. Sea P cualquier polinomio distinguido en Λ que sea primo relativo a $f \cdot g$. Para ver su existencia, notemos que, por el criterio de Eisenstein, $T^n + p$ es distinguido e irreducible para toda n . Puesto que hay una infinidad de ellos, existe uno que es primo relativo a fg .

Si $(x, y) \in N$, entonces $p^i(x, y) \cong p^j(x, y) \text{ mód } M$ para algunos $i < j$. Puesto que $1 - p^{j-i} \in \Lambda^*$, entonces

$$\begin{aligned} p^i(x, y) &= (1 - p^{j-i})^{-1}(1 - p^{j-i})p^i(x, y) = \\ &= (1 - p^{j-i})^{-1}(p^i(x, y) - p^j(x, y)) \in M. \end{aligned}$$

Por lo tanto $p^k N \subseteq M$ para algún k (recordemos que $|N/M| < \infty$). Supongamos $p^k(x, y) = 0$ en N . Entonces $f|p^k x$, $g|p^k y$. Puesto que $\text{mcd}(p, fg) = 1$, entonces $f|x$ y $g|y$ lo cual implica que $(x, y) = 0$ en N . Se sigue que si $\cdot p^k$ denota multiplicación por p^k , entonces

$$N \xrightarrow{\cdot p^k} M \xrightarrow{\sim} \Lambda/\langle f, g \rangle \text{ es inyectivo.}$$

La imagen contiene al ideal $\langle p^k, fg \rangle$ y puesto que p^k y fg son primos relativos, se sigue que $\Lambda/\langle p^k fg \rangle$ es finito y por lo tanto conúcleo($\cdot p^k$) es finito. \square

Proposición 13.6.11. *Los ideales primos de Λ son (0) , $\langle p, T \rangle$, $\langle p \rangle$ y $\langle P(T) \rangle$ donde $P(T)$ es un polinomio distinguido irreducible. Más aún, Λ es un anillo local con ideal maximal $\langle p, T \rangle$.*

Demostración. Se tienen los siguientes isomorfismos

$$\begin{aligned} \Lambda/(0) &\cong \Lambda, \\ \Lambda/\langle p \rangle &\cong \mathbb{F}_p[[T]], \\ \Lambda/\langle p, T \rangle &\cong \mathbb{F}_p, \\ \Lambda/\langle P(T) \rangle &\cong \mathbb{Z}_p[T]/\langle P(T) \rangle, \end{aligned}$$

este último isomorfismo se puede obtener usando el algoritmo euclideo. Puesto que todos los cocientes anteriores son dominios enteros, todos los ideales son primos y además contenidos en $\langle p, T \rangle$.

Sea ahora \mathfrak{p} un ideal primo no cero de Λ . Sea $h \in \mathfrak{p}$ de grado mínimo. Sea $h = p^s H$ con $H = 1$ o H distinguido. Puesto que \mathfrak{p} es primo se sigue que $p \in \mathfrak{p}$ o $H \in \mathfrak{p}$. En el caso en que $1 \neq H \in \mathfrak{p}$, entonces, puesto que h es de grado mínimo, H necesariamente es irreducible. En cualquier de estos dos casos, $\langle f \rangle \subseteq \mathfrak{p}$ donde $f = p$ o f es irreducible y distinguido. Si $\langle f \rangle = \mathfrak{p}$ el resultado se sigue. Si $\langle f \rangle \neq \mathfrak{p}$, consideremos $g \in \mathfrak{p}$, $g \notin \langle f \rangle$, esto es, $f \nmid g$.

Puesto que f es irreducible, f y g son primos relativos y $\langle f, g \rangle \subseteq \mathfrak{p}$ implica que $|\Lambda/\mathfrak{p}| \leq |\Lambda/\langle f, g \rangle| < \infty$. En particular Λ/\mathfrak{p} es un \mathbb{Z}_p -módulo finito y $p^{n_0} \in \mathfrak{p}$ para alguna $n_0 \in \mathbb{N}$ y como \mathfrak{p} es primo, $p \in \mathfrak{p}$.

Por otro lado, tenemos que $T^i \equiv T^j \pmod{\mathfrak{p}}$ para algunos $i, j \in \mathbb{N}$, $i < j$ y ya que $1 - T^{j-i} \in \Lambda^*$, entonces

$$T^i = (1 - T^{j-i})^{-1}(T^i(1 - T^{j-i})) = (1 - T^{j-i})^{-1}(T^i - T^j) \in \mathfrak{p}$$

lo que a su vez implica que $T \in \mathfrak{p}$ y por lo tanto $\langle p, T \rangle \subseteq \mathfrak{p}$. Finalmente, puesto que $\Lambda/\langle p, T \rangle \cong \mathbb{F}_p$ se sigue que $\langle p, T \rangle$ es maximal y por lo tanto $\langle p, T \rangle = \mathfrak{p}$. \square

En contraste a la finitud de $\Lambda/\langle f, g \rangle$ (Lema 13.6.9) se tiene:

Proposición 13.6.12. *Sea $f \in \Lambda$, $f \notin \Lambda^*$. Entonces $\Lambda/\langle f \rangle$ es infinito.*

Demostración. Supongamos $f \neq 0$ pues de otra manera el resultado es inmediato. Por el Teorema de Preparación de Weierstrass, basta suponer que $f = p$ o $f = P(T)$ con $P(T)$ un polinomio distinguido. Si $f = p$, $\Lambda/\langle p \rangle \cong \mathbb{F}_p[[T]]$ y si $f = P(T)$ es un polinomio distinguido, $\Lambda/\langle f \rangle = \Lambda/\langle P(T) \rangle \cong \mathbb{Z}_p[T]/\langle P(T) \rangle$ el cual es isomorfo, como grupo, a $\mathbb{Z}_p^{\text{gr}_T P(T)}$. El resultado se sigue. \square

Definición 13.6.13. Dos Λ -módulos M y M' se llaman *seudo-isomorfos*, lo cual denotamos por $M \sim M'$, si existe un Λ -homomorfismo $\varphi: M \rightarrow M'$ tal que tanto $\text{núc } \varphi$ como $\text{conúcleo } \varphi$ son conjuntos finitos.

Equivalentemente, M y M' son pseudo isomorfos si existe una sucesión exacta de Λ -módulos

$$0 \longrightarrow A \longrightarrow M \longrightarrow M' \longrightarrow B \longrightarrow 0$$

con A y B finitos.

Observación 13.6.14. Si $M \sim M'$, no necesariamente $M' \sim M$. En particular, \sim no es una relación de equivalencia.

Ejemplo 13.6.15. Se tiene que $\langle p, T \rangle \sim \Lambda$ pues la inyección natural $\langle p, T \rangle \rightarrow \Lambda$ tiene conúcleo \mathbb{F}_p el cual es finito.

Por otro lado, si $\varphi: \Lambda \rightarrow \langle p, T \rangle$ es cualquier Λ -homomorfismo, sea $\varphi(1) = f(T)$. Entonces se tiene que $\text{conúcleo } \varphi = \langle p, T \rangle / \langle f \rangle$. Puesto que $|\Lambda/\langle f \rangle| = \infty$ y $|\Lambda/\langle p, T \rangle| < \infty$, necesariamente $|\langle p, T \rangle / \langle f \rangle| = \infty$.

Sin embargo, lo que si se tiene es:

Teorema 13.6.16. *Si M y M' son Λ -módulos de torsión finitamente generados, entonces $M \sim M' \iff M' \sim M$.*

Demostración. Ver [75, pág. 272]. \square

Observación 13.6.17. Si $f, g \in \Lambda$ son primos relativos, entonces por el casi Teorema Chino del Residuo, $\Lambda/\langle fg \rangle \sim \Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle$ y $\Lambda/\langle f \rangle \oplus \Lambda/\langle g \rangle \sim \Lambda/\langle fg \rangle$.

Teorema 13.6.18 (Estructura de Λ -módulos finitamente generados). *Sea M un Λ -módulo finitamente generado. Entonces*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/\langle p^{n_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/\langle f_j(T)^{m_j} \rangle \right)$$

donde $r, s, t, n_i, m_j \in \mathbb{N} \cup \{0\}$ y cada $f_j(T)$ es un polinomio irreducible distinguído.

Demostración. El enunciado es similar al de la estructura de un módulo sobre un dominio de ideales principales, pero en nuestro caso tenemos únicamente un pseudo-isomorfismo en lugar de un isomorfismo.

Supongamos que M está generado por u_1, \dots, u_n con relaciones $\lambda_1 u_1 + \dots + \lambda_n u_n = 0$, $\lambda_i \in \Lambda$.

Sea R el Λ -submódulo de Λ^n formado por las relaciones. Puesto que Λ es un anillo noetheriano, R es Λ -finitamente generado. Así M puede ser representado por una matriz cuyas filas son de la forma $(\lambda_1, \dots, \lambda_n)$ y donde $\sum_{i=1}^n \lambda_i u_i = 0$ es una relación. Se tiene la sucesión exacta $0 \longrightarrow R \longrightarrow \Lambda^n \longrightarrow M \longrightarrow 0$ de Λ -módulos. Por abuso del lenguaje, esta matriz también será llamada R .

Las siguientes son las operaciones básicas de filas y columnas que corresponden a cambiar generadores de R y M .

Operación A: Permuta de filas o de columnas.

Operación B: Adicionamos un múltiplo de una fila o una columna a otra fila o columna respectivamente. Como caso especial, si $\lambda' = q\lambda + r$,

$$\begin{pmatrix} \vdots & \vdots & \vdots \\ \lambda & \dots & \lambda' & \dots \\ \vdots & & \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots & \vdots & \vdots \\ \lambda & \dots & r & \dots \\ \vdots & & \vdots \end{pmatrix} \quad r = \lambda' - q\lambda.$$

Operación C: Podemos multiplicar una fila o una columna por un elemento de Λ^* .

Notemos que estas tres operaciones son las mismas que las usadas para los dominios de ideales principales. Tendremos tres operaciones adicionales que es donde intervienen los pseudos-isomorfismos en lugar de los isomorfismos.

Operación 1: Si R contiene una fila $(\lambda_1, p\lambda_2, \dots, p\lambda_n)$ con $p \nmid \lambda_1$ entonces cambiamos R por la matriz R' cuya primer fila es $(\lambda_1, \lambda_2, \dots, \lambda_n)$ y las demás filas de R' son las filas de R con el primer elemento multiplicado por p :

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots & \cdots \\ \alpha_1 & \alpha_2 & \cdots & \cdots \\ \beta_1 & \beta_2 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \cdots \\ p\alpha_1 & p\alpha_2 & \cdots & \cdots \\ p\beta_1 & p\beta_2 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

Como caso especial, si $\lambda_2 = \cdots = \lambda_n = 0$, entonces podemos multiplicar α_1, β_1, \dots por una potencia arbitraria de p .

Afirmamos que el módulo M' es pseudo-isomorfo a M . En efecto, en R tenemos la relación

$$\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n) = 0$$

Sea $\tilde{M}' = M \oplus Av$ con un nuevo generador v y sean las relaciones adicionales $(-u_1, pv) = 0$, $(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0$. Sea M' igual a \tilde{M}' módulo estas nuevas relaciones.

Sea $M \xrightarrow{\varphi} M'$ el mapeo natural. Si $m \in \text{nuc } \varphi$, m está en el módulo de relaciones así que:

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v), \quad a, b \in A$$

de donde $ap = -b\lambda_1$. Puesto que $p \nmid \lambda_1$, $p|b$ y $\lambda_1|a$. En la primera componente obtenemos

$$\begin{aligned} m &= -a_1 u_1 + b(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= \frac{-a}{\lambda_1}(\lambda_1, u) - \frac{ap}{\lambda_1}(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\frac{a}{\lambda_1}(\lambda_1 u_1 + p\lambda_2 u_2 + \cdots + p\lambda_n u_n) = -\frac{a}{\lambda_1}(0) = 0 \end{aligned}$$

lo cual prueba que φ es inyectiva.

Ahora bien las imágenes de $pv = "u_1$ y $\lambda_1 v = " - (\lambda_2 u_2 + \cdots + \lambda_n u_n)$ en M' están en la imagen de M y el ideal $\langle p, \lambda_1 \rangle$ aniquila a M'/M . Puesto que $p \nmid \lambda_1$, $\text{mcd}(p, \lambda_1) = 1$, $|A/\langle p, \lambda_1 \rangle| < \infty$ y M' es finitamente generado, se sigue que $|M'/M| < \infty$ y por tanto $M \sim M'$.

El nuevo módulo tiene generadores v, u_2, \dots, u_n , " $u_1 = pv$ ". Cualquier relación $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0$ viene a ser $p\alpha_1 v + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0$. Así que la primer columna es multiplicada por p . Finalmente también tenemos la relación $\lambda_1 v + \lambda_2 u_2 + \cdots + \lambda_n u_n = 0$ así que la nueva matriz R' tiene la forma dada pues removemos la fila redundante $(p\lambda_1, p\lambda_2, \dots, p\lambda_n)$.

Continuamos con la demostración del teorema.

Operación 2: Si todos los elementos de la primer columna de R son divisibles por p^k y si existe una fila $(p^k \lambda_1, \dots, p^k \lambda_n)$ con $p \nmid \lambda_1$, podemos cambiar

R a una matriz R' que es la misma que R excepto que $(p^k \lambda_1, \dots, p^k \lambda_n)$ es reemplazado por $(\lambda_1, \dots, \lambda_n)$. Es decir

$$\begin{pmatrix} p^k \lambda_1 & p^k \lambda_2 & \cdots & \cdots \\ p^k \alpha_1 & \alpha_2 & \cdots & \cdots \\ p^k \beta_1 & \beta_2 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \cdots \\ p^k \alpha_1 & \alpha_2 & \cdots & \cdots \\ p^k \beta_1 & \beta_2 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Al hacer esto obtenemos un módulo M' tal que $M' = M'' \oplus S$, donde M'' está dado por la matriz R' y $S \cong \Lambda/\langle p^k \rangle$ para algún k . Por lo tanto, como veremos a continuación, S es de la forma de los sumandos directos del enunciados del teorema y $M \sim M'$.

Se tiene $M' = (M \oplus \Lambda v) / \langle (p^k u_1, -p^k v), (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) \rangle$. Como en la Operación 1, puesto que $p \nmid \lambda_1$, podemos encajar M en M' y también el ideal $\langle p^k, \lambda_1 \rangle$ aniquila a M'/M . Por lo tanto $|M'/M| < \infty$ y $M \sim M'$.

Ahora bien, usando que $p^k(u_1 - v) = 0$ y que p^k divide al primer coeficiente entre las relaciones que involucran a u_1 , se tiene que $M' = M'' \oplus \Lambda(u_1 - v)$ donde M'' está generado por v, u_2, \dots, u_n y tiene relaciones generadas por $(\lambda_1, \dots, \lambda_n)$ y R . Por tanto M'' tiene R' por relación. Notemos que $\Lambda(u_1 - v) \cong \Lambda/\langle p^k \rangle$ que es de la forma de la suma directa buscada.

Operación 3: Si R contiene una fila $(p^k \lambda_1, \dots, p^k \lambda_n)$ y para algún λ con $p \nmid \lambda$, $(\lambda \lambda_1, \dots, \lambda \lambda_n)$ es también una relación, no necesariamente explícitamente contenida en R , entonces podemos cambiar R a R' , donde R' es la misma que R excepto que $(p^k \lambda_1, \dots, p^k \lambda_n)$ se reemplaza por $(\lambda_1, \dots, \lambda_n)$. Veamos que el módulo M' obtenido es pseudo isomorfo a M .

Para probar nuestra afirmación, consideremos $\varphi: M \rightarrow M' := M/\Lambda(\lambda_1 u_1 + \cdots + \lambda_n u_n)$ la proyección canónica. Se tiene que núc φ es aniquilado por el ideal $\langle \lambda, p^k \rangle$. Puesto que M es finitamente generado, núc φ es finitamente generado y $\Lambda/\langle \lambda, p^k \rangle$ es finito si y sólo si núc φ es finito. Puesto que φ es suprayectiva, $M \sim M'$ y M' tiene la matriz de relaciones R' .

Las seis operaciones A, B, C, 1, 2 y 3 se llaman *admisibles* y todas ellas conservan las dimensiones de la matriz original.

Continuando con la demostración del teorema, sea $f \in \Lambda \setminus \{0\}$. Entonces por el Teorema de Preparación de Weierstrass, tenemos $f(T) = p^u P(T)U(T)$ con $P(T)$ un polinomio distinguido y $U \in \Lambda^*$. Definimos

$$\text{gr}_\omega f := \begin{cases} \infty & \text{si } \mu > 0 \\ \text{gr } P & \text{si } \mu = 0 \end{cases}.$$

$\text{gr}_\omega f$ se llama el *grado de Weierstrass de f* . Dada una matriz R definimos

$$\text{gr}^{(k)} R := \min \text{gr}_\omega(a'_{i,j}) \quad \text{para } i, j \geq k$$

donde $(a'_{i,j})$ recorre todo el conjunto de matrices obtenidas a partir de R por medio de operaciones admisibles que dejan las primeras $(k-1)$ filas sin cambio.

Permitimos que $a_{i,j}$ cambie para $i \geq k$ y cualquier j . También permitimos operaciones del tipo B que usa, pero que no cambia, las primeras $(k-1)$ filas.

Si la matriz R tiene la forma

$$\begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & * & \cdots & * & * & \cdots & * \\ * & * & \cdots & * & * & \cdots & * \end{pmatrix} := \begin{pmatrix} D_{r-1} & 0 \\ M & N \end{pmatrix}$$

con $\lambda_{k,k}$ un polinomio distinguido y $\text{gr } \lambda_{k,k} = \text{gr}_\omega \lambda_{k,k} = \text{gr}^{(k)}(R)$ para $1 \leq k \leq r-1$, decimos que R está en la forma $(r-1)$ -normal.

Antes de continuar la demostración del teorema, probemos

Lema 13.6.19. *Si la submatriz N es no cero, entonces R puede ser transformada con operaciones admisibles en una matriz R' que está en la forma r -normal y que tiene los primeros $(r-1)$ elementos diagonales iguales a los de R .*

Demostración (Lema 13.6.19). Usando la Operación 1, podemos suponer, en caso necesario, que una potencia grande de p divide cada $\lambda_{i,j}$ con $i \geq r$ y $j \leq r-1$, es decir, los elementos de M .

Esto es, $p^t | M$, para t suficientemente grande y tal que $p^t \nmid N$. Usando la Operación 2, podemos suponer $p \nmid N$. Así mismo, podemos suponer que N tiene una entrada $\lambda_{i,j}$ tal que $\text{gr}_\omega \lambda_{i,j} = \text{gr}^{(r)} R < \infty$.

Si $\lambda_{i,j} = P(T)U(T)$ con $P(T)$ polinomio distinguido y $U(T) \in A^*$, multipliquemos la columna j por U^{-1} . De esta forma podemos suponer que $\lambda_{i,j}$ es distinguido puesto que las primeras $r-1$ filas tienen 0 en la columna j , y por lo tanto esos elementos no cambian. Por la Operación A, podemos suponer $\lambda_{ij} = \lambda_{rr}$ nuevamente por la razón que tenemos 0 en los primeros lugares.

Por el algoritmo de la división, el cual es un caso especial de la Operación B, podemos suponer que λ_{rj} es un polinomio con $\text{gr } \lambda_{rj} < \text{gr } \lambda_{rr}$, $j \neq r$ y $\text{gr } \lambda_{rj} < \text{gr } \lambda_{jj}$, $j < r$.

Ahora bien λ_{rr} tiene grado de Weierstrass minimal en N por lo que se debe tener que $p | \lambda_{rj}$ para $j > r$. Por la Operación 1, podemos suponer que $p^t | \lambda_{rj}$, $j > r$, t suficientemente grande. Si $\lambda_{rj} \neq 0$ para algún $j > r$, por la Operación 1, podemos quitar la potencia de p de algún λ_{rj} con $j > r$ y los ceros siguen sin cambios alguno. Tenemos

$$\text{gr}_\omega \lambda_{rj} \leq \text{gr } \lambda_{rj} < \text{gr } \lambda_{rr} = \text{gr}_\omega \lambda_{jj}$$

lo cual es imposible. Consecuentemente, $\lambda_{rj} = 0$ para $j > r$.

Si $\lambda_{rj} \neq 0$ para $j < r$ por la Operación 1 podemos obtener $p \nmid \lambda_{rj}$ para alguna j , pero en este caso se tiene

$$\text{gr}_\omega \lambda_{rj} \leq \text{gr } \lambda_{rj} < \text{gr } \lambda_{jj} = \text{gr}_\omega \lambda_{jj}$$

y ya que $\text{gr}_\omega \lambda_{jj} = \text{gr}^{(j)}(R)$ se obtiene una contradicción a la definición de $\text{gr}^{(j)}(R)$. De esto concluimos que $\lambda_{rj} = 0$ para todo $j \neq r$ que es lo que queríamos probar. \square

Continuamos con la demostración del teorema. Por el Lema 13.6.19 empezamos con la matriz con $r = 1$ y podemos ir cambiando R hasta obtener una matriz

$$\left(\begin{array}{ccc|c} \lambda_{11} & & 0 & \\ & \ddots & & 0 \\ 0 & & \lambda_{rr} & \\ \hline & M & & 0 \end{array} \right)$$

con cada λ_{jj} un polinomio distinguido y $\text{gr} \lambda_{jj} = \text{gr}^{(j)} R$ para $j \leq r$. Por el algoritmo de la división podemos suponer λ_{ij} es un polinomio y que $\text{gr} \lambda_{ij} < \text{gr} \lambda_{jj}$ para $i \neq j$. Si tuviésemos $\lambda_{ij} \neq 0$ para algún $i \neq j$, puesto que $\text{gr}_\omega \lambda_{jj}$ es minimal, necesariamente $p | \lambda_{ij}$ y por ende tenemos una relación no cero $(\lambda_{i1}, \dots, \lambda_{ir}, 0, \dots, 0)$ que es divisible por p . Sea $\lambda := \lambda_{11} \cdots \lambda_{rr}$. Entonces p no divide a λ y puesto que λ_{jj} es un polinomio distinguido para $j = 1, \dots, r$, se tiene que

$$\left(\lambda \frac{1}{p} \lambda_{i1}, \dots, \lambda \frac{1}{p} \lambda_{ir}, 0, \dots, 0 \right)$$

también es una relación puesto que $\lambda_{jj} u_j = 0$.

Por la Operación 3, podemos suponer que P no divide a λ_{ij} para algún j , así que $\text{gr}_\omega \lambda_{ij} \leq \text{gr} \lambda_{ij} < \text{gr} \lambda_{jj} = \text{gr}^{(j)} R$ lo cual es imposible. Por lo tanto $\lambda_{ij} = 0$ para todo i, j tales que $i \neq j$. Esto significa que $M = 0$.

En términos de A -módulos, tenemos:

$$M' = A/\langle \lambda_{11} \rangle \oplus A/\langle \lambda_{22} \rangle \oplus \cdots \oplus A/\langle \lambda_{rr} \rangle \oplus A^{n-r}.$$

Volviendo a escribir los factores $A/\langle p^k \rangle$ que quitamos durante la Operación 2 obtenemos el resultado con la salvedad de que λ_{ii} no necesariamente es una potencia de un polinomio irreducible, pero puesto que si f y g son primos relativos tenemos

$$A/\langle f, g \rangle \sim A/\langle f \rangle \oplus A/\langle g \rangle \quad \text{y} \quad A/\langle f \rangle \oplus A/\langle g \rangle \sim A/\langle f, g \rangle$$

esto termina la demostración del teorema. \square

13.7. Los invariantes de Iwasawa

Nuestro objetivo en esta sección es probar lo siguiente: Sea K un campo numérico finito y sea $K_\infty/K_0 = K$ una extensión \mathbb{Z}_p . Si p^{e_n} es la potencia

exacta de p que divide al número de clase de K_n , $h(K_n)$, entonces existen enteros no negativos $\lambda \geq 0$, $\mu \geq 0$ y un entero γ , independientes de n y un número natural n_0 tal que para $n \geq n_0$,

$$e_n = \mu p^n + \lambda n + \gamma. \quad (13.1)$$

Definición 13.7.1. Los números μ, λ, γ dados en (13.1) se llaman los *invariantes de Iwasawa*.

Sea K_∞/K una extensión \mathbb{Z}_p , $\Gamma = \text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ y sea γ_0 un generador topológico de Γ . Sea L_n la máxima p -extensión abeliana no ramificada de K_n . Se tiene que $X_n := \text{Gal}(L_n/K_n) \cong A_n$, donde A_n es el p -subgrupo de Sylow del grupo de clases $\mathcal{Cl}(K_n)$ del campo K_n .

$$\begin{array}{ccccc} L_0 & \text{---} & L_n & \text{---} & L \\ \downarrow A_0 & & \downarrow A_n & & \\ K = K_0 & \text{---} & K_n & \text{---} & K_\infty \end{array}$$

Sea $L := \bigcup_{n=1}^{\infty} L_n$. Notemos que $L_n \subseteq L_{n+1}$ ya que $K_{n+1}L_n/K_{n+1}$ es una extensión no ramificada.

Sea $X := \text{Gal}(L/K_\infty)$. Puesto que L_n es maximal, se tiene que L_n/K es una extensión de Galois y por lo tanto es una extensión de Galois. Sea $G := \text{Gal}(L/K)$. Se tiene la sucesión exacta $1 \rightarrow X \rightarrow G \rightarrow \Gamma \rightarrow 1$.

$$\begin{array}{c} L \\ \swarrow X \\ K_\infty \\ \downarrow \Gamma \\ K \end{array} \quad \begin{array}{c} \nearrow G \\ \nearrow \end{array}$$

Definición 13.7.2. La condición (A) se define por:

(A) Todos los primos ramificados de K_∞/K son totalmente ramificados.

Observación 13.7.3. Como vimos anteriormente (Proposición 13.5.7), si K_∞/K no satisface la condición (A), existen un número natural m tal que K_∞/K_m es totalmente ramificado en cada primo ramificado y por lo tanto K_∞/K_m satisface la condición (A).

Supondremos que K_∞/K satisface la condición (A). Entonces L_n/K_n es no ramificada y K_{n+1}/K_n es totalmente ramificada por lo que $K_{n+1} \cap L_n = K_n$ lo cual implica que $\text{Gal}(L_n/K_n) \cong \text{Gal}(L_n K_{n+1}/K_{n+1}) \cong \frac{\text{Gal}(L_{n+1}/K_{n+1})}{\text{Gal}(L_{n+1}/L_n K_{n+1})}$. Por lo tanto $X_n \cong \frac{X_{n+1}}{\text{Gal}(L_{n+1}/L_n K_{n+1})}$.

Se tiene el mapeo restricción suprayectivo: $X_{n+1} \xrightarrow{\text{rest}} X_n$. Se tiene el siguiente resultado de la Teoría de Campos de Clase:

Teorema 13.7.4. Si L/K y L'/K' son dos extensiones abelianas de campos numéricos tales que $K \subseteq K'$ y $L \subseteq L'$. Entonces tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} I_{K'} & \xrightarrow{[\cdot, L'|K']} & \text{Gal}(L'/K') \\ \downarrow N_{K'/K} & & \downarrow \text{rest} \\ I_K & \xrightarrow{[\cdot, L|K]} & \text{Gal}(L/K) \end{array}$$

donde I_K e $I_{K'}$ son los grupos ya sea de divisores o de idèles de K y K' respectivamente, $N_{K'/K}$ es la norma de $I_{K'}$ a I_K ; $[\cdot, L|K]$ y $[\cdot, L'|K']$ son los mapeos de Artin y $\text{rest}: \text{Gal}(L'/K') \rightarrow \text{Gal}(L/L \cap K') \subseteq \text{Gal}(L/K)$, $\sigma \mapsto \sigma|_L$, es el mapeo restricción.

Demostración. Sea \mathfrak{p} un ideal de K' no ramificado en L'/K' y sea \mathfrak{P} un ideal de L' sobre \mathfrak{p} . Similarmente, sean $\tilde{\mathfrak{p}}$, $\tilde{\mathfrak{P}}$ para L y K de tal forma que $\tilde{\mathfrak{p}} = \mathfrak{p}|_K$, $\tilde{\mathfrak{P}} = \mathfrak{P}|_L$, $\tilde{\mathfrak{p}}$ no ramificado en L/K .

$$\begin{array}{ccccc} \mathfrak{p} & - & - & K' & \xrightarrow{\quad} & K'L & \xrightarrow{\quad} & L' & - & - & \mathfrak{P} \\ & & & \downarrow & & \downarrow & & & & & \\ \tilde{\mathfrak{p}} & - & - & K & \xrightarrow{\quad} & L & - & - & - & \tilde{\mathfrak{P}} \end{array}$$

Sea $f = [\mathcal{O}_{K'}/\mathfrak{p} : \mathcal{O}_K/\tilde{\mathfrak{p}}]$ el grado relativo. Entonces $N_{K'/K}\mathfrak{p} = \tilde{\mathfrak{p}}^f$ y si N es la norma absoluto, $N\mathfrak{p} = (N\tilde{\mathfrak{p}})^f$. Puesto que $\mathcal{O}_L \subseteq \mathcal{O}_{L'}$, se tiene

$$\sigma_{\mathfrak{p}}^{L'/K'} := [\mathfrak{p}, L'|K'] \quad \text{y} \quad \sigma_{\mathfrak{p}}^{L'/K'}|_L(x) \equiv x^{N\mathfrak{p}} \pmod{\tilde{\mathfrak{P}}} \quad \text{para} \quad x \in \mathcal{O}_L.$$

Ahora

$$\begin{aligned} \sigma_{N_{K'/K}\mathfrak{p}}^{L/K}(x) &= [N_{K'/K}\mathfrak{p}, L|K](x) = [\tilde{\mathfrak{p}}, L/K]^f(x) \\ &\equiv x^{(N\tilde{\mathfrak{p}})^f} = x^{N\mathfrak{p}} \pmod{\tilde{\mathfrak{P}}} \quad \text{para} \quad x \in \mathcal{O}_L. \end{aligned}$$

Por lo tanto

$$\begin{aligned} \text{rest}[\cdot, L'|K'](\mathfrak{P}) &= \text{rest} \circ [\mathfrak{P}, L'|K'] = [N_{K'/K}\mathfrak{P}, L|K] \\ &= ([\cdot, L|K] \circ N_{K'/K})(\mathfrak{P}). \end{aligned} \quad \square$$

Aplicando el Teorema 13.7.4, tenemos el diagrama conmutativo

$$\begin{array}{ccc} X_{n+1} & \xrightarrow{\text{rest}} & X_n \\ \downarrow [\cdot, L_{n+1}|K_{n+1}] \cong & & \cong \downarrow [\cdot, L_n|K_n] \\ A_{n+1} & \xrightarrow{N_{K_{n+1}/K_n}} & A_n \end{array}$$

corresponde a la norma: $A_{n+1} \rightarrow A_n$ sobre el grupo de clases. Ahora bien, $\text{Gal}(L_n K_\infty / K_\infty) \cong \text{Gal}(L_n / L_n \cap K_\infty = K_n) \cong X_n$. Por tanto

$$\begin{aligned} \varprojlim_n X_n &\cong \varprojlim_n \text{Gal}(L_n K_\infty / K_\infty) = \text{Gal}\left(\left(\bigcup_{n=1}^{\infty} L_n K_\infty\right) / K_\infty\right) \\ &= \text{Gal}(L / K_\infty) \cong X. \end{aligned}$$

Esto es, $\varprojlim_n X_n = \varprojlim_n \text{Gal}(L_n / K_n) \cong \text{Gal}(L / K_\infty) \cong X$.

Sea $\gamma \in \Gamma_n = \Gamma / \Gamma^{p^n}$ y extendamos γ a $\tilde{\gamma} \in \text{Gal}(L_n / K)$. Sea $x \in X_n$. Entonces γ actúa en x por: $x^\gamma := \tilde{\gamma} x \tilde{\gamma}^{-1}$.

$$\begin{array}{ccc} & L_n & \\ & \swarrow & \downarrow X_n \\ K & \xrightarrow{\Gamma_n} & K_n \end{array} \quad 1 \longrightarrow X_n \longrightarrow \text{Gal}(L_n / K) \longrightarrow \Gamma_n \longrightarrow 1.$$

Puesto que $X_n = \text{Gal}(L_n / K_n)$ es abeliano, x^γ está bien definida pues si γ' es tal que $\tilde{\gamma}(\tilde{\gamma}')^{-1} \in X_n$, entonces

$$(\tilde{\gamma}^{-1}(\tilde{\gamma}'))x(\tilde{\gamma}^{-1}\tilde{\gamma}')^{-1} = x \quad \text{por lo que} \quad \tilde{\gamma}'x\tilde{\gamma}'^{-1} = \tilde{\gamma}x\tilde{\gamma}^{-1}.$$

Esta acción corresponde a la acción de Γ_n en A_n ya que $\left[\frac{L|K}{\sigma\mathfrak{p}}\right] = \sigma\left[\frac{L|K}{\mathfrak{p}}\right]\sigma^{-1}$. Esto es, X_n es un $\mathbb{Z}_p[\Gamma_n]$ -módulo. Si representamos un elemento $X \cong \varprojlim_n X_n$ como un vector (x_0, x_1, \dots) y dejando $\mathbb{Z}_p[\Gamma_n]$ actuar en la n -ésima componente, entonces X es un Λ -módulo, $\Lambda = \varprojlim_n \mathbb{Z}_p[\Gamma_n]$: si $\mathbf{x} \in X$ y $\boldsymbol{\lambda} \in \Lambda$, $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \dots)$, $\mathbf{x}^{\boldsymbol{\lambda}} := (\tilde{\lambda}_0 x_0 \tilde{\lambda}_0^{-1}, \tilde{\lambda}_1 x_1 \tilde{\lambda}_1^{-1}, \dots, \tilde{\lambda}_n x_n \tilde{\lambda}_n^{-1}, \dots)$. Ahora $\tilde{\lambda}_{n+1} x_{n+1} \tilde{\lambda}_{n+1}^{-1} \xrightarrow{\text{rest}} \tilde{\lambda}_{n+1}|_{K_n} x_{n+1}|_{K_n} \tilde{\lambda}_{n+1}^{-1}|_{K_n} = \tilde{\lambda}_n x_n \tilde{\lambda}_n^{-1}$, por lo tanto $\mathbf{x}^{\boldsymbol{\lambda}} \in X$.

Con el isomorfismo $\Lambda \cong \mathbb{Z}_p[[T]]$, $1 + T \in \Lambda$ actúa como $\gamma_0 \in \Gamma$. Se tiene $x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1}$ para $\gamma \in \Gamma$, $x \in X$ y $\tilde{\gamma}$ es una extensión de γ a G .

Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ los primos ramificados en K_∞ / K y sean $\tilde{\mathfrak{p}}_1, \dots, \tilde{\mathfrak{p}}_s$ primos de L sobre cada \mathfrak{p}_i . Sean $I_i \subseteq G$ los grupos de inercia de $\tilde{\mathfrak{p}}_i$, $1 \leq i \leq s$.

Puesto que L / K_∞ es no ramificada, $I_i \cap X = \{1\}$. Puesto que K_∞ / K es totalmente ramificado en \mathfrak{p}_i , se tiene que el mapeo $I_i \hookrightarrow G / X \cong \Gamma$ es suprayectivo y por tanto un isomorfismo. De esta forma tenemos que $G = I_i X = X I_i$, $1 \leq i \leq s$. Sea $\sigma_i \in I_i$ el elemento que se mapea a γ_0 . Entonces σ_i es un generador topológico de I_i . Puesto que $I_i \subseteq X I_1$, se tiene que existe $a_i \in X$ tal que $\sigma_i = a_i \sigma_1$, y $a_1 = 1$.

$$\begin{array}{ccc} & L & \\ & \swarrow X & \\ K_\infty & & \\ \Gamma \downarrow & & \\ K & & \end{array}$$

Proposición 13.7.5. *Si la extensión K_∞/K satisface la condición (A), entonces si G' es la cerradura del subgrupo conmutador de G , se tiene $G' = X^{\gamma_0-1} = TX$.*

Demostración. Puesto que $\Gamma \cong I_1 \subseteq G$, y I_1 se mapea sobre $\Gamma \cong G/X$, se puede levantar γ al correspondiente elemento en I_1 para así definir la acción de Γ en X . Por simplicidad, identificamos Γ y I_1 de tal manera que $x^\gamma = \gamma x \gamma^{-1}$. Sea $a = \alpha x$, $b = \beta y$ con $\alpha, \beta \in \Gamma$ y $x, y \in X$ elementos arbitrarios de $G = \Gamma X$. Entonces

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} \underbrace{(\alpha\beta)\alpha^{-1}}_{\in \Gamma} y^{-1} \beta^{-1} \stackrel{\Gamma \text{ abeliano}}{=} x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \\ &\stackrel{X \text{ abeliano}}{=} x^\alpha (x^{-1})^{\alpha\beta} y^{\alpha\beta} (y^{-1})^\beta = (x^\alpha)^{1-\beta} (y^\beta)^{\alpha-1} \in G'. \end{aligned}$$

Tomemos $\beta = 1$, $\alpha = \gamma_0$, entonces $(x^\alpha)^0 y^{\gamma_0-1} = y^{\gamma_0-1} \in G'$, esto es, $X^{\gamma_0-1} \subseteq G'$.

Para $\beta \in \Gamma$ arbitrario, existe $c \in \mathbb{Z}_p$ tal que $\beta = \gamma_0^c$. Por tanto

$$1 - \beta = 1 - \gamma_0^c = (1 - (1+T)^c) = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda$$

donde $\binom{c}{n} := \frac{c(c-1)\cdots(c-n+1)}{n!}$, $n \in \mathbb{N} \cup \{0\}$. Puesto que $\gamma_0 - 1 = T$, $(x^\alpha)^{1-\beta} \in X^{\gamma_0-1}$.

Similarmente obtenemos que $(y^\beta)^{1-\alpha} \in X^{\gamma_0-1}$. Finalmente, puesto que $X^{\gamma_0-1} = TX$ es cerrado por ser la imagen de conjunto compacto X , se sigue que $G' \subseteq X^{\gamma_0-1}$ y por ende $G' = X^{\gamma_0-1}$. \square

Proposición 13.7.6. *Sea K_∞/K que satisface la condición (A). Sea Y_0 el \mathbb{Z}_p submódulo de X generado por $\{a_i \mid 2 \leq i \leq s\}$ y por $X^{\gamma_0-1} = TX$ donde tenemos $\sigma_i = a_i \sigma_1$, $\overline{\langle \sigma_1 \rangle} = I_i$. Sea $Y_n := \gamma_n Y_0$, donde*

$$\gamma_n := 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n-1} = \frac{\gamma_0^{p^n} - 1}{\gamma_0 - 1} = \frac{(1+T)^{p^n} - 1}{T}.$$

Entonces $X_n \cong X/Y_n$ para $n \geq 0$.

Demostración. Primero sea $n = 0$. Se tiene $K \subseteq L_0 \subseteq L$ y L_0 es la máxima p -extensión abeliana no ramificada de K . Entonces $\text{Gal}(L/L_0)$ es el subgrupo cerrado de G generado por G' , pues L_0/K es abeliana, y por todos los subgrupos de inercia I_i , $1 \leq i \leq s$ ya que L_0/K es no ramificada. Por lo tanto $\text{Gal}(L/L_0)$ es el subgrupo cerrado generado por X^{γ_0-1} , I_1 y a_2, \dots, a_s de tal forma que

$$\begin{aligned} X_0 = \text{Gal}(L_0/K) &= \frac{G}{\text{Gal}(L/L_0)} = \frac{XI_1}{\text{Gal}(L/L_0)} \\ &\cong \frac{I_1X}{\langle X^{\gamma_0-1}, I_1, a_2, \dots, a_2 \rangle} \cong \frac{X}{\langle X^{\gamma_0-1}, a_2, \dots, a_2 \rangle} = \frac{X}{Y_0}. \end{aligned}$$

Consideremos $n \geq 1$, Reemplazando K por K_n y γ_0 por $\gamma_0^{p^n}$ se tiene que $\sigma_i^{p^n}$ toma el papel de σ_i . Se sigue que

$$\begin{array}{ccccc} & & L_n & \text{---} & L \\ & & \downarrow X_n & & \downarrow \\ K & \text{---} & K_n & \text{---} & K_\infty \end{array}$$

$$\begin{aligned} \sigma_i^{k+1} &= (a_i \sigma_1)^{k+1} = a_i \sigma_1 a_i \sigma_1^{-1} \sigma_1^2 a_i \sigma_1^{-2} \sigma_1^3 \cdots \sigma_1^k a_i \sigma_1^{-k} \sigma_1^{k+1} \\ &= a_i^{1+\sigma_1+\cdots+\sigma_1^k} \sigma_i^{k+1}. \end{aligned}$$

Por tanto $\sigma_i^{p^n} \underset{\sigma_1=\gamma_0}{=} (\gamma_n a_i) \sigma_1^{p^n}$, esto es, a_i es reemplazado por $\gamma_n a_i$.

Finalmente X^{γ_0-1} es reemplazado por $X^{\gamma_0^{p^n}-1} = \gamma_n X^{\gamma_0-1}$ y Y_0 es reemplazado por $\gamma_n Y_0$ lo cual implica el resultado. \square

Observación 13.7.7. La Proposición 13.7.6 es crucial pues nos permite recabar información para X_n de la información que se tenga de X .

Veamos un resultado básico de álgebra conmutativa aplicado a nuestro caso (ver Teorema 13.2.6).

Proposición 13.7.8 (Lema de Nakayama). *Sea X un Λ -módulo compacto, es decir, X tiene una topología compacta Hausdorff, X es un Λ -módulo y la acción de Λ en X ; $\Lambda \times X \rightarrow X$, es una función continua.*

Entonces X es finitamente generado como Λ -módulo si y solamente si $X/\langle p, T \rangle X$ es finito.

Si x_1, \dots, x_n generan $X/\langle p, T \rangle X$ sobre \mathbb{Z} , entonces x_1, \dots, x_n generan X como Λ -módulo. En particular

$$X/\langle p, T \rangle X = 0 \iff X = 0.$$

Demostración. Sea U una vecindad abierta de $0 \in X$. Puesto que $\langle p, T \rangle^n \rightarrow 0$ en Λ , cada $z \in X$ tiene una vecindad abierta U_z tal que $\langle p, T \rangle^{n_z} U_x \subseteq U$ para algún $n_z \in \mathbb{N}$ suficientemente grande. Puesto que X es compacto, un número finito de las vecindades U_z cubren a X . En particular, para n suficientemente grande, $\langle p, T \rangle^n X \subseteq U$ y por tanto

$$\bigcap_{n=1}^{\infty} (\langle p, T \rangle^n X) = \{0\}.$$

Ahora bien, $\Lambda/\langle p, T \rangle \cong \mathbb{F}_p$ es finito y $X/\langle p, T \rangle X$ es un $\Lambda/\langle p, T \rangle$ -módulo, de donde se sigue que $X/\langle p, T \rangle X$ es finitamente generado si y solamente si es finito.

Sean x_1, \dots, x_n generadores $X/\langle p, T \rangle X$ y sea $Y = \Lambda x_1 + \dots + \Lambda x_n \subseteq X$. Puesto que Y es imagen continua de Λ^n , Y es un conjunto compacto y por lo tanto Y es cerrado en X . Se sigue que X/Y es un Λ -módulo compacto. Tenemos

$$\langle p, T \rangle(X/Y) = \frac{T + \langle p, T \rangle X}{Y} = \frac{X}{Y}$$

de donde se sigue que $\langle p, T \rangle^n(X/Y) = X/Y$ para toda $n \geq 0$. Por lo tanto $X/Y = \bigcap_{n=0}^{\infty} \langle p, T \rangle^n(X/Y) = \{0\}$ y por lo tanto $X = Y$, esto es, $\{x_1, \dots, x_n\}$ genera a X . \square

Proposición 13.7.9. *Si la extensión K_∞/K satisface la condición (A) y $X = \text{Gal}(L/K_\infty)$, entonces X es un Λ -módulo finitamente generado.*

Demostración. Se tiene $\gamma_1 = 1 + \gamma_0 + \dots + \gamma_0^{p-1} \in \langle p, T \rangle$, por lo que $Y_0/\langle p, T \rangle Y_0$ es cociente de $Y_0/\gamma_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$ donde $Y_0 = \langle X^{\gamma_0^{-1}}, a_2, \dots, a_s \rangle$, $Y_n = \gamma_n Y_0$, $X_n \cong X/Y_n$.

Puesto que X_1 es finito, Y_0 es finitamente generado. Por otro lado, $X/Y_0 = X_0$ es finito lo cual implica que X es finitamente generado como Λ -módulo. \square

Ahora analicemos el caso en que K_∞/K no necesariamente satisface la condición (A). Sea $e \geq 0$ tal que en K_∞/K_e todos los primos ramificados son totalmente ramificados. Los resultados anteriores se satisfacen para K_∞/K_e . En particular X , el cual es el mismo tanto para K como para K_e , es finitamente generado como Λ -módulo. Para $n \geq e$ tenemos

$$1 = \gamma_0^{p^e} + \gamma_0^{2p^e} + \dots + \gamma_0^{p^n - p^e} = \frac{\gamma_n}{\gamma_e} =: \gamma_{n,e},$$

$$\text{de hecho, } \frac{\gamma_n}{\gamma_e} = \frac{\gamma_0^{p^n} - 1}{\gamma_0^{p^e} - 1} = \frac{(\gamma_0^{p^e})^{p^{n-e}} - 1}{\gamma_0^{p^e} - 1}.$$

Entonces $\gamma_{n,e}$ reemplaza γ_n en la extensión K_∞/K_e puesto que $\gamma_0^{p^e}$ es un generador topológico de $\text{Gal}(K_\infty/K_e)$. Sea Y_e el respectivo módulo Y_0 para K_e en lugar de K . Entonces $Y_n = \gamma_{n,e} Y_e$ y $X_n = X/Y_n$ para $n \geq e$. Entonces tenemos

Proposición 13.7.10. *Sea K_∞/K una extensión \mathbb{Z}_p . Entonces se tiene que $X := \text{Gal}(L/K_\infty)$ es un Λ -módulo finitamente generado y existe $e \geq 0$ tal que $X_n \cong X/\gamma_{n,e} Y_e$ para toda $n \geq e$. \square*

Podemos aplicar el teorema de estructura de Λ -módulos finitamente generados para X y para Y_e y puesto que X/Y_e es finito, se tiene que

$$Y_e \sim X \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda / \langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda / \langle f_j(T)^{m_j} \rangle \right). \quad (13.2)$$

Calcularemos $V/\gamma_{n,e}V$ para cada sumando del pseudo isomorfismo dado en (13.2).

- (1) Si $V = \Lambda$ se tiene que $\Lambda / \langle \gamma_{n,e} \rangle$ es infinito. Puesto que $Y_e / \gamma_{n,e} Y_e \subseteq X / Y_n$ es finito, se sigue que Λ no puede aparecer como sumando, esto es, $r = 0$ en (13.2) y X es de torsión.
- (2) Si $V = \Lambda / \langle p^k \rangle$, entonces $V / \gamma_{n,e} V = \Lambda / \langle p^k, \gamma_{n,e} \rangle$.
Se tiene que

$$\begin{aligned} \gamma_{n,e} &= \frac{\gamma_n}{\gamma_e} = \frac{((1+T)^{p^n} - 1)/T}{((1+T)^{p^e} - 1)/T} \\ &= 1 + (1+T)^{p^e} + (1+T)^{2p^e} + \cdots + (1+T)^{p^n - p^e} \end{aligned}$$

es un polinomio distinguido.

Ahora, por el algoritmo de la división, se tiene que cada elemento de $\Lambda / \langle p^k, \gamma_{n,e} \rangle$ se representa unívocamente por un polinomio módulo p^k de grado menor a $\text{gr } \gamma_{n,e} = p^n - p^e$. Por lo tanto

$$|V / \gamma_{n,e} V| = p^{k(p^n - p^e)} = p^{kp^n + c}$$

donde c es la constante $c = -kp^e$.

- (3) $V = \Lambda / \langle f(T)^m \rangle$ donde $f(T)$ es un polinomio distinguido e irreducible. Sea $g(T) := f(T)^m$. Entonces g también es un polinomio distinguido, digamos de grado d . Entonces

$$T^d \equiv pQ(T) \pmod{g}$$

para algún $Q(T) \in \mathbb{Z}_p[T]$. Por lo tanto $T^k \equiv (p)S \pmod{g}$, S es un polinomio, $k \geq d$. Así, si $p^n \geq d$, se tiene

$$(1+T)^{p^n} = 1 + (p)S_1 + T^{p^n} \equiv 1 + (p)S_2 \pmod{g}$$

con S_1, S_2 polinomios.

Por lo tanto $(1+T)^{p^{n+1}} \equiv 1 + p^2 S_3 \pmod{g}$, S_3 un polinomio. En general se sigue que

$$\begin{aligned} P_{n+2}(T) &:= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1)((1+T)^{p^{n+1}} - 1) \\ &\equiv (1 + \cdots + 1 + p^2 S_4) P_{n+1}(T) \equiv p(1 + pS_5) P_{n+1}(T) \pmod{g} \end{aligned}$$

donde S_4, S_5 son polinomios.

Ahora bien, $1 + pS_6 \in \Lambda^*$, para S_6 polinomio, se tiene que $\frac{P_{n+2}}{P_{n+1}}$ actúa como multiplicación pu , $u \in \Lambda^*$ sobre $V = \Lambda/\langle g(T) \rangle$ para $p^n \geq d$. Supongamos $n_0 > e$, $p^{n_0} \geq d$ y $n \geq n_0$. Entonces

$$\frac{\gamma_{n+2,e}}{\gamma_{n+1,e}} = \frac{\gamma_{n+2}}{\gamma_{n+1}} = \frac{P_{n+2}}{P_{n+1}} \quad \text{y} \quad \gamma_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(\gamma_{n+1,e}V) = p\gamma_{n+1,e}V.$$

Por tanto

$$|V/\gamma_{n+2,e}V| = |V/pV| |pV/p\gamma_{n+1,e}V| \quad \text{para} \quad n \geq n_0.$$

Puesto que $\text{mcd}(g(T), p) = 1$, se tiene que multiplicación por p es inyectiva en donde obtenemos

$$|pV/p\gamma_{n+1,e}V| = |V/\gamma_{n+1,e}V| \quad \text{para} \quad n \geq n_0.$$

Puesto que $V/pV = \Lambda/\langle p, g(T) \rangle = \Lambda/\langle p, T^d \rangle$ se sigue que $|V/pV| = p^d$. Por inducción en n , obtenemos

$$|V/\gamma_{n,e}V| = p^{d(n-n_0-1)} |V/\gamma_{n_0+1,e}V|, \quad n \geq n_0 + 1.$$

Si $V/\gamma_{n,e}V$ es finito para toda n , entonces $|V/\gamma_{n,e}V| = p^{dn+c}$ para $n \geq n_0 + 1$ y alguna constante c . Si $V/\gamma_{n,e}V$ es infinito, V no puede ser sumando en el pseudo isomorfismo (13.2) debido a que $|Y_e/\gamma_{n,e}Y_e| < \infty$. Este caso puede suceder únicamente cuando $\text{mcd}(\gamma_{n,e}, f) \neq 1$.

Resumimos toda la discusión anterior en:

Teorema 13.7.11. *Sea $E = \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/\langle g_j(T) \rangle \right)$ donde cada $g_j(T)$ es un polinomio distinguido, no necesariamente irreducible. Sea $m := \sum_{i=1}^s k_i$, $\ell = \sum_{j=1}^t \text{gr } g_j(T)$. Si $E/\gamma_{n,e}E$ es finito para toda n , entonces $r = 0$ y existen $n_0 \in \mathbb{N}$ y $c \in \mathbb{Z}$ tales que para $n > n_0$, $|E/\gamma_{n,e}E| = p^{mp^n + \ell n + c}$. \square*

Teorema 13.7.12. *Sea E como en el Teorema 13.7.11 con $r = 0$. Entonces se tiene que $m = 0$ si y solamente si el p -rango de $E/\gamma_{n,e}E$ permanece acotado cuando $n \rightarrow \infty$.*

Demostración. Si A es un grupo abeliano finito, tenemos que el p -rango de A es igual a $\dim_{\mathbb{F}_p} A/pA$. Ahora bien, recordemos que $\gamma_{n,e}$ es distinguido de grado $p^n - p^e$, así, si $\text{gr } \gamma_{n,e} \geq \max_{1 \leq j \leq t} \text{gr } g_j(T)$, se tiene que

$$\begin{aligned}
E/\gamma_{n,e}E &= \left(\bigoplus_{i=1}^s \Lambda/\langle p, \gamma_{n,e} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/\langle p, g_j(T), \gamma_{n,e} \rangle \right) \\
&\cong \left(\bigoplus_{i=1}^s \Lambda/\langle p, T^{p^n - p^e} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/\langle p, T^{\text{gr } g_j(T)} \rangle \right) \\
&\cong (\mathbb{Z}/p\mathbb{Z})^{s(p^n - p^e) + \ell}.
\end{aligned}$$

Por tanto, el p -rango de E está acotado si y solamente si $s = 0$ si y solamente si $m = 0$. \square

Regresando a la extensión K_∞/K , tenemos una sucesión exacta:

$$0 \longrightarrow A \longrightarrow Y_e \longrightarrow E \longrightarrow B \longrightarrow 0$$

donde A y B son finitos y E es como antes. Conocemos $|E/\gamma_{n,e}E|$ para $n > n_0$. De aquí ya podemos concluir que si p^n es la potencia exacta que divide a $|A_n| = |X_n| = \left| \frac{X}{\gamma_{n,e}Y_e} \right|$ se tiene $e_n = mp^n + \ell n + c_n$ con c_n acotado.

La siguiente pieza es:

Proposición 13.7.13. *Sean Y y E Λ -módulos pseudo isomorfos de tal forma que $Y/\gamma_{n,e}Y$ es finito para $n \geq e$. Entonces existen una constante c y alguna n_0 tales que $|Y/\gamma_{n,e}Y| = p^c |E/\gamma_{n,e}E|$ para toda $n \geq n_0$.*

Demostración. Se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \gamma_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/\gamma_{n,e}Y \longrightarrow 0 \\
& & \downarrow \phi'_n & & \downarrow \phi & & \downarrow \phi''_n \\
0 & \longrightarrow & \gamma_{n,e}E & \longrightarrow & E & \longrightarrow & E/\gamma_{n,e}E \longrightarrow 0
\end{array}$$

Se tiene:

- (I) Puesto que $\text{núc } \phi'_n \subseteq \text{núc } \phi$, $|\text{núc } \phi'_n| \leq |\text{núc } \phi|$.
- (II) Se tiene $\text{conúcleo } \phi = E/\Phi(Y)$. Sea $E/\Phi(Y) = \{\bar{u}_1, \dots, \bar{u}_r\}$. Es decir, si $x \in E$, es tal que $x \equiv u_i \pmod{\Phi(Y)}$, se tiene que $\gamma_{n,e}x - \gamma_{n,e}u_i \in \gamma_{n,e}\Phi(Y) = \Phi(\gamma_{n,e}Y)$ lo cual implica que $\frac{\gamma_{n,e}E}{\Phi(\gamma_{n,e}Y)} = \{\overline{\gamma_{n,e}u_1}, \dots, \overline{\gamma_{n,e}u_r}\}$ y por lo tanto $|\text{conúcleo } \phi'_n| \leq |\text{conúcleo } \phi|$.
- (III) Puesto que los representantes de $\text{conúcleo } \phi$ dan representantes de $\text{conúcleo } \phi''_n$ se sigue que $|\text{conúcleo } \phi''_n| \leq |\text{conúcleo } \phi|$.
- (IV) Aplicando el Lema de la Serpiente, se tiene la sucesión exacta

$$\begin{aligned}
0 &\longrightarrow \text{núc } \phi'_n \longrightarrow \text{núc } \phi \longrightarrow \text{núc } \phi''_n \longrightarrow \\
&\longrightarrow \text{conúcleo } \phi'_n \longrightarrow \text{conúcleo } \phi \longrightarrow \text{conúcleo } \phi''_n \longrightarrow 0.
\end{aligned}$$

Por tanto $|\text{núc } \phi''_n| \leq |\text{núc } \phi| |\text{conúcleo } \phi'_n|$ y por (II)

$$|\text{núc } \phi| |\text{conúcleo } \phi'_n| \leq |\text{núc } \phi| |\text{conúcleo } \phi|.$$

Esto es $|\text{núc } \phi''_n| \leq |\text{núc } \phi| |\text{conúcleo } \phi|$.

Ahora bien, si $m \geq n \geq 0$, tenemos

(a) $|\text{núc } \phi'_n| \geq |\text{núc } \phi'_m|$:

Se tiene $\gamma_{m,e} = \frac{\gamma_{m,e}}{\gamma_{n,e}} \gamma_{n,e}$, por lo que $\gamma_{m,e}Y \subseteq \gamma_{n,e}Y$ y por ende $\text{núc } \phi'_m \subseteq \text{núc } \phi'_n$.

(b) $|\text{conúcleo } \phi'_n| \geq |\text{conúcleo } \phi'_m|$:

Sean $\gamma_{m,e}y \in \gamma_{m,e}E$ y $z \in \gamma_{n,e}E$ el representante del elemento $\gamma_{n,e}y$ en $\text{conúcleo } \phi'_n = \frac{\gamma_{n,e}E}{\gamma_{n,e}\phi'_n(Y)}$. Por tanto $\gamma_{n,e}y - z = \phi(\gamma_{n,e}x)$ para algún $x \in Y$. Multiplicando por $\frac{\gamma_{m,e}}{\gamma_{n,e}}$, se tiene que

$$\gamma_{m,e}y - \left(\frac{\gamma_{m,e}}{\gamma_{n,e}}\right)(z) = \phi(\gamma_{m,e}x) = \phi'_n(\gamma_{m,e}x).$$

Es decir, los representantes de $\text{conúcleo } \phi'_m$ se obtienen de multiplicar los representantes de $\text{conúcleo } \phi'_n$ por $\frac{\gamma_{m,e}}{\gamma_{n,e}}$.

(c) $|\text{conúcleo } \phi''_n| \leq |\text{conúcleo } \phi''_m|$:

Se tiene que $\gamma_{m,e}E \subseteq \gamma_{n,e}E$. Por lo tanto, del epimorfismo $E/\gamma_{m,e}E \rightarrow E/\gamma_{n,e}E$ se tiene que $\text{conúcleo } \phi''_n \twoheadrightarrow \text{conúcleo } \phi''_m$.

Obtenemos $|\text{núc } \phi'_m| \underset{(a)}{\leq} |\text{núc } \phi'_n| \underset{(i)}{\leq} |\text{núc } \phi|$ para $m \geq n$,

$$\begin{aligned} |\text{conúcleo } \phi'_m| &\underset{(b)}{\leq} |\text{conúcleo } \phi'_n| \underset{(ii)}{\leq} |\text{conúcleo } \phi| \quad \text{y} \\ |\text{conúcleo } \phi''_n| &\underset{(c)}{\leq} |\text{conúcleo } \phi''_m| \underset{(iii)}{\leq} |\text{conúcleo } \phi''|. \end{aligned}$$

Por tanto existe $n_0 \in \mathbb{N}$ tal que para $n \geq n_0$ los órdenes de $\text{núc } \phi'_n$, $\text{conúcleo } \phi'_n$ y $\text{conúcleo } \phi''_n$ son constantes.

Finalmente, por el Lema de la Serpiente, tenemos que

$$|\text{núc } \phi'_n| |\text{núc } \phi''_n| |\text{conúcleo } \phi| = |\text{núc } \phi| |\text{conúcleo } \phi'_n| |\text{conúcleo } \phi''_n|$$

por lo que $|\text{núc } \phi''_n|$ es constante para $n \geq n_0$. Así, para toda $n \geq n_0$, tenemos

$$0 \longrightarrow \text{núc } \phi''_n \longrightarrow Y/\gamma_{n,e}Y \xrightarrow{\phi''} E/\gamma_{n,e}E \longrightarrow \text{conúcleo } \phi''_n \longrightarrow 0$$

lo cual implica que $|Y/\gamma_{n,e}Y| = \frac{|\text{núc } \phi''_n|}{|\text{conúcleo } \phi''_n|} |E/\gamma_{n,e}E|$. □

Teorema 13.7.14 (Iwasawa). *Sea M un Λ -módulo finitamente generado de torsión y supongamos que para $n \in \mathbb{Z}$, $n \geq 0$, $M/\gamma_n M$ es un grupo finito de orden p^{e_n} . Entonces existen enteros no negativos m , ℓ , y un entero c tales que para n suficientemente grande, $e_n = mp^n + \ell n + c$.*

Demostración. Sea $M \sim A^r \oplus \left(\bigoplus_{i=1}^s A/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t A/\langle f_j^{m_j}(T) \rangle \right)$. Puesto que $|M/\gamma_n M| < \infty$, $r = 0$ y por la Proposición 13.7.13 se tiene $|M/\gamma_n M| = p^{mp^n + \ell n + c}$ con $m = \sum_{i=1}^s k_i$, $\ell = \sum_{j=1}^t m_j \text{ gr } f_j(T)$ y $c \in \mathbb{Z}$. \square

Como caso especial, obtenemos el resultado principal:

Teorema 13.7.15 (Iwasawa). *Sea K_∞/K una extensión \mathbb{Z}_p . Sea p^{e_n} la potencia exacta que divide al número de clase de K_n . Entonces existen enteros $\lambda \geq 0$, $\mu \geq 0$ y γ independientes de n , y un natural n_0 tal que para $n \geq n_0$, $e_n = \mu p^n + \lambda n + \gamma$.* \square

Teorema 13.7.16. *Sea K_∞/K una extensión \mathbb{Z}_p en la cual exactamente un primo es ramificado y este es totalmente ramificado. Entonces*

$$Cl_{K_n}(p) = A_n \cong X_n \cong \frac{X}{((1+T)^{p^n} - 1)}$$

y $p \nmid h_0 \iff p \nmid h_n$ para toda $n \geq 0$, donde $h_n = |Cl_{K_n}(p)|$.

Demostración. Se tiene que K_∞/K satisface la condición (A) con $s = 1$, es decir, un único primo ramificado. Entonces

$$Y_0 = \langle TX = X^{\gamma_0-1}, a_2, \dots, a_s \rangle = TX,$$

$$Y_n = \gamma_n Y_0 = \frac{(1+T)^{p^n} - 1}{T} Y_0 = ((1+T)^{p^n} - 1)X.$$

Por tanto $X_n \cong X/Y_n = \frac{X}{((1+T)^{p^n} - 1)X}$.

Si $p \nmid h_0$, entonces $X/TX = X/Y_0 \cong A_0 = \{1\}$, esto es, $X/TX = 0$ lo cual implica $X/\langle p, T \rangle X = 0$. Por el Lema de Nakayama, $X = 0$ y $A_n = \{1\}$ para toda $n \geq 0$. \square

Corolario 13.7.17. *Para $K = \mathbb{Q}$ y p cualquier primo, $\mu = \lambda = \gamma = 0$.*

Demostración. Se tiene que $\mathbb{Q}_\infty/\mathbb{Q}$ es una extensión \mathbb{Z}_p de \mathbb{Q} y $h_0 = |Cl_{\mathbb{Q}}| = 1$. Puesto que únicamente p se ramifica, $A_n = \{1\}$ para toda n , esto es, $|A_n| = p^{e_n}$, $e_n = 0 = \mu p^n \lambda n + \gamma$. \square

Teorema 13.7.18. *Se tiene que $\mu = 0$ si y sólo si el p -rango de A_n se mantiene acotado cuando $n \rightarrow \infty$.*

Demostración. Se tiene $Y_e \sim E = \left(\bigoplus_{i=1}^s A/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t A/\langle f_j^{m_j}(T) \rangle \right)$. Se tiene que $s = 0$ si y solamente si el p -rango de $E/\gamma_{n,e}E$ está acotado. Como antes, tenemos una sucesión exacta

$$0 \longrightarrow C_n \longrightarrow Y_e/\gamma_{n,e}Y_e \longrightarrow E/\gamma_{n,e}E \longrightarrow B_n \longrightarrow 0$$

con $|C_n|$, $|B_n|$ acotados para toda n . Por lo tanto $\mu = 0$ si y solamente si el p -rango de $Y_e/\gamma_{n,e}Y_e$ está acotado. Se tiene $A_n \cong X_n = X/\gamma_{n,e}Y_e$ y X/Y_e es finito. El resultado se sigue. \square

Conjetura 13.7.19 (Iwasawa). Si K es cualquier campo numérico finito y K_∞/K es la extensión \mathbb{Z}_p -ciclotómica de K , entonces $\mu = 0$.

Iwasawa primero conjeturó esto para cualquier extensión \mathbb{Z}_p . Sin embargo él mismo encontró contraejemplos cuando K_∞/K no es la extensión ciclotómica. Washington y Ferrero probaron la Conjetura 13.7.19 cuando K/\mathbb{Q} es una extensión abeliana.

Ahora bien, tenemos

Teorema 13.7.20. *Se tiene que $\lambda = 0$ si y solamente si el exponente de A_n está acotado.*

Demostración.

\Rightarrow) Sea $X \sim E = \left(\bigoplus_{i=1}^s \Lambda/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/\langle f_j(T)^{m_j} \rangle \right)$. Entonces $\mu = \sum_{i=1}^s k_i$, $\lambda = \sum_{j=1}^t m_j \operatorname{gr} f_j(T)$. Se tiene

$$\lambda = 0 \iff X \sim \bigoplus_{i=1}^s \Lambda/\langle p^{k_i} \rangle.$$

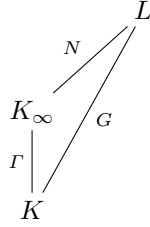
Sea $k_0 = \max_{1 \leq i \leq s} k_i$, entonces $p^{k_0}X \sim 0$, es decir, $p^{k_0}X$ es finito, por lo que existe $a \in \mathbb{N}$ tal que $p^a X = \{0\}$ lo cual implica que $p^a A_n \cong p^a X_n = 0$, es decir, el exponente de A_n está acotado.

\Leftarrow) Sea $p^a A_n = 0$ para alguna $a \in \mathbb{N}$ y toda n . Entonces $p^a X_n = p^a(X/\gamma_{n,e}Y_e) = 0$ para $n \geq e$. Por lo tanto $p^a X \subseteq \bigcap_{n=e}^{\infty} \gamma_{n,e}Y_e = \{0\}$, esto es, $t = 0$ pues para toda $f(T) \neq 0$ distinguido e irreducible se tiene $p^a(\Lambda/\langle f(T)^m \rangle) \neq 0$. Por lo tanto $\lambda = 0$. \square

Conjetura 13.7.21 (R. Greenberg). Sea K un campo numérico finito. Si K es totalmente real, es decir, $r_2 = 0$, entonces $\lambda = \mu = 0$.

Proposición 13.7.22. *Sea K un campo numérico finito, K_∞/K una extensión \mathbb{Z}_p y s el número de divisores primos de K ramificados en K_∞/K . Sea L/K_∞ una p -extensión de K_∞ no ramificada tal que L/K es abeliana. Entonces $\operatorname{Gal}(L/K) \cong \mathbb{Z}_p^t \oplus R$ donde R es un p -grupo finito y $t \leq s$.*

Demostración.



Sean $G := \text{Gal}(L/K)$ y $N := \text{Gal}(L/K_\infty)$. Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ los primos de K ramificados en K_∞/K y sean T_1, \dots, T_s los respectivos grupos de inercia de cada \mathfrak{p}_i en L/K . Puesto que L/K_∞ es no ramificada se tiene que $T_i \cap N = \{0\}$ para $i = 1, \dots, s$. Por lo tanto $T_i \cong T_i N/N$, esto es, T_i es isomorfo a un subgrupo cerrado no trivial de $\Gamma = G/N$. Se tiene que $T_i \cong \Gamma$ para $1 \leq i \leq s$.

Sean $T := T_1 \cdots T_s$, $E = L^T$ y $\text{Gal}(L/E) = T$. Se tiene que E/K es no ramificada y abeliana y por ende finita, esto es G/T es un grupo finito. Ahora bien, G/T es un p -grupo debido a que tanto G como T son \mathbb{Z}_p -módulos.

Así, $T \cong \mathbb{Z}_p^t \oplus R_1$ con R_1 un p -grupo finito y $t \leq s$ ya que $T = T_1 \cdots T_s$ y $T_i \cong \Gamma$, $1 \leq i \leq s$. Por lo tanto $G \cong \mathbb{Z}_p^t \oplus R$ con R un p -grupo finito. \square

Corolario 13.7.23. Si $s = 1$, es decir, únicamente hay un primo ramificado, entonces la máxima p -extensión no ramificada L de K_∞ tal que L/K es abeliana satisface que L/K_∞ es finita.

Demostración. Se tiene en este caso que $G \cong \mathbb{Z}_p^t \oplus R$, $1 \leq t \leq 1 = s$ y $\text{Gal}(K_\infty/K) \cong \Gamma$, por lo que $R = \text{Gal}(L/K_\infty)$ es un p -grupo finito. \square

Observación 13.7.24. Ya habíamos probado que si F es la máxima extensión abeliana K no ramificada fuera de p , entonces $\text{Gal}(F/K) \cong \mathbb{Z}_p^{r_2+1+\delta} \times$ (finito) (ver Teorema 13.5.11).

Definición 13.7.25. Un campo numérico K se llama de tipo MC (*multiplicación compleja*) si K es totalmente imaginario que es una extensión cuadrática de un campo totalmente real.

Ejemplo 13.7.26. Si $K \not\subseteq \mathbb{R}$ y K/\mathbb{Q} es una extensión abeliana, entonces para todo encaje $\sigma: K \rightarrow \mathbb{C}$, $\sigma(K) = K \not\subseteq \mathbb{R}$ por lo que K es totalmente imaginario. Sea $J: K \rightarrow K$, $x \mapsto \bar{x}$ la conjugación compleja. Entonces $J \in \text{Gal}(K/\mathbb{Q})$ y $o(J) = 2$ pues $J|_K \neq \text{Id}_K$. Sea $K^+ := K^{\{1, J\}} = K \cap \mathbb{R}$. Entonces K es totalmente real pues $K^+ \subseteq \mathbb{R}$ y K^+/\mathbb{Q} es de Galois. Finalmente $[K : K^+] = |\{1, J\}| = 2$. Por tanto K es de tipo MC.

Ejemplo 13.7.27. Si $n \geq 3$, $\mathbb{Q}(\zeta_n)$ es un campo de tipo MC.

Proposición 13.7.28. Si K es de tipo MC y si K^+ es su subcampo real, esto es, $[K : K^+] = 2$ y K^+ es totalmente real, entonces la conjugación compleja J induce un automorfismo en K el cual es independiente del encaje K en \mathbb{C} . Además $K^+ = K \cap \mathbb{R}$.

Demostración. Sean $\phi, \psi: K \rightarrow \mathbb{C}$ dos encajes de K . Notemos que $\phi(K)/\phi(K^+)$ es una extensión cuadrática y por tanto normal. Además, puesto que $\phi(K^+) \subseteq \mathbb{R}$, entonces $J(\phi(K^+)) = \phi(K^+)$, es decir, $J \circ \phi(\alpha) = \phi(\alpha)$ para todo $\alpha \in K^+$. Sea $\bar{\phi} := J \circ \phi$. Puesto que $\phi(K)/\phi(K^+)$ es normal, se tiene $J(\phi(K)) = \phi(K)$,

es decir, $\bar{\phi}(K) = \phi(K)$. Se sigue que $\phi^{-1} \circ \bar{\phi}$ está definida en K . De esta forma tenemos que $\psi^{-1} \circ \bar{\psi}$ y $\phi^{-1} \circ \bar{\phi}$ son automorfismos de K que fijan a K^+ puesto que K^+ es totalmente real.

Ahora bien, puesto que K es totalmente imaginario, ni $\phi^{-1} \circ \bar{\phi}$ ni $\psi^{-1} \circ \bar{\psi}$ puede ser la identidad y puesto que $\text{Gal}(K/K^+)$ es de orden 2 se sigue que $\phi^{-1} \circ \bar{\phi} = \psi^{-1} \circ \bar{\psi} = J$. Por lo tanto $J: K \rightarrow K$ es un automorfismo de K , $J \neq \text{Id}$ y $\text{Gal}(K/K^+) = \{1, J\}$. Finalmente $K^+ = K^{\{1, J\}} = K \cap \mathbb{R}$. \square

Observación 13.7.29. Dado un campo numérico finito, $[K : K \cap \mathbb{R}]$ puede ser arbitrariamente grande. Por ejemplo, si $K = \mathbb{Q}(\zeta_n \sqrt[3]{2})$, se tiene que $K \cap \mathbb{R} = \mathbb{Q}$ y $[K : \mathbb{Q}] = n$. Otro ejemplo es si $p \geq 3$ un número primo y sea $f(x) = x^{2p} + 3$. Si $\omega_0, \dots, \omega_{2p-1}$ son las raíces de $f(x)$, $\omega_t = 3^{1/2p} e^{((\pi+2t\pi)i)/2p}$.

Tomemos por ejemplo $\omega_0 = 3^{1/2p} e^{\pi i/2p}$ y sea $K := \mathbb{Q}(\omega_0)$. Entonces $[K : \mathbb{Q}] = 2p$ y K es totalmente imaginario pues si $\sigma: K \rightarrow \mathbb{C}$ es un encaje, $\mathbb{Q}(\omega_0) \longrightarrow \mathbb{Q}(\zeta_p, \omega_0) \quad \sigma(K) = \mathbb{Q}(\omega_i)$ para alguna i , $0 \leq i \leq 2p-1$.
 $\left. \begin{array}{c} \text{Por otro lado, la cerradura de Galois de } K/\mathbb{Q} \\ \text{es } \tilde{K} := \mathbb{Q}(\zeta_{2p}, \omega_0) = \mathbb{Q}(\zeta_p, \omega_0). \text{ Se tiene que} \\ \mathbb{Q}(\zeta_{2p}, \omega_0)/\mathbb{Q}(\zeta_{2p}) \text{ es una extensión de Kummer} \\ \text{cíclica de grado } 2p. \text{ Sea } A := \mathbb{Q}(\omega_0) \cap \mathbb{R}. \end{array} \right\}^{2p}$
 $\mathbb{Q} \longrightarrow \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$

Notemos que en general si $[K : K \cap \mathbb{R}] = 2$ entonces necesariamente $\text{Gal}(K/K \cap \mathbb{R}) = \{1, J\}$, esto es, $K^J = K$.

Por tanto si tuviésemos $[\mathbb{Q}(\omega_0) : A] = 2$, entonces $A = \mathbb{Q}(\omega_0^2)$ puesto que hay una correspondencia entre los subcampos de $\mathbb{Q}(\omega_0)$ que contienen a \mathbb{Q} y los de $\mathbb{Q}(\omega_0, \zeta_{2p})$ que contienen a $\mathbb{Q}(\zeta_{2p})$ y esta última es cíclica.

En particular hay un único subcampo de índice 2 en $\mathbb{Q}(\omega_0)$ y por tanto este corresponde a $\mathbb{Q}(\omega_0^2)$. Sin embargo $\omega_0^2 = 3^{1/p} e^{\pi i/p} \notin \mathbb{R}$. Todos los subcampos de $\mathbb{Q}(\omega_0)$ son $\mathbb{Q}(\omega_0^j)$, con $j = 0, 1, \dots, 2p-1$ y $\omega_0^j = 3^{j/2p} e^{\pi j i/2p} \in \mathbb{R} \iff j = 2p$. En particular

$$\mathbb{Q}(\omega_0) \cap \mathbb{R} = \mathbb{Q} \quad \text{y} \quad [\mathbb{Q}(\omega_0) : \mathbb{Q}(\omega_0) \cap \mathbb{R}] = [\mathbb{Q}(\omega_0) : \mathbb{Q}] = 2p.$$

Teorema 13.7.30. Sea K un campo numérico finito de tipo MC y sea $K^+ := K \cap \mathbb{R}$ su subcampo real. Sean $h := |\text{Cl}(K)|$, $h^+ = |\text{Cl}(K^+)|$. Entonces $h^+ | h$.

Demostración.

Se tiene que K/K^+ es totalmente ramificado en todos los primos arquimideanos de K^+ . Sean H_K y H_{K^+} los campos de clase de Hilbert de K y K^+ respectivamente. Entonces $K \cap H_{K^+} = K^+$ pues H_{K^+}/K^+ es no ramificada. Por tanto $H_{K^+}K/K$ es una extensión abeliana y no ramificada. Se sigue que $H_{K^+}K \subseteq H_K$. Obtenemos que

$$\begin{array}{ccc} H_{K^+} & \longrightarrow & H_{K^+}K \\ \downarrow & & \downarrow \\ K^+ & \longrightarrow & K \end{array}$$

$$\begin{aligned} h &= |\text{Cl}(K)| = [H_K : K] = [H_K : H_{K^+}K][H_{K^+}K : K] \\ &= [H_K : H_{K^+}K][H_{K^+} : K^+] = [H_K : H_{K^+}K]|\text{Cl}(K^+)| \\ &= [H_K : H_{K^+}K]h^+. \end{aligned}$$

\square

Teorema 13.7.31. Sea K un campo de tipo MC y sea E el grupo de unidades de K . Sea E^+ el grupo de unidades de K^+ y sea W el grupo de raíces de unidad en K . Entonces si definimos $Q = [E : WE^+]$, se tiene que $Q = 1$ o 2 .

Demostración. Sea $\phi: E \rightarrow W$ definida por $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$. Puesto que para todo encaje $\sigma: K \rightarrow \mathbb{C}$ se tiene que $\overline{\varepsilon^\sigma} = \bar{\varepsilon}^\sigma$ se sigue que

$$|\phi(\varepsilon)^\sigma| = |(\varepsilon/\bar{\varepsilon})^\sigma| = |\varepsilon^\sigma/\bar{\varepsilon}^\sigma| = \left| \frac{\varepsilon^\sigma}{\bar{\varepsilon}^\sigma} \right| = 1$$

lo cual implica que $\phi(\varepsilon) \in W$. Sea $\psi: E \rightarrow W/W^2$ el mapeo inducido por ϕ , es decir, el mapeo $\pi \circ \phi$ donde π es la proyección natural $W \rightarrow W/W^2$

$$E \xrightarrow{\phi} W \xrightarrow{\pi} W/W^2.$$

Supongamos que $\varepsilon = \xi\varepsilon_1$ con $\xi \in W$, $\varepsilon_1 \in E^+$, entonces

$$\phi(\varepsilon) = \phi(\xi\varepsilon_1) = \frac{\xi\varepsilon_1}{\bar{\xi}\bar{\varepsilon}_1} = \frac{\xi}{\bar{\xi}} = \frac{\xi}{\xi^{-1}} = \xi^2 \in W^2.$$

En particular $\varepsilon \in \text{núc } \psi$.

Recíprocamente, si $\varepsilon \in \text{núc } \psi$, entonces $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon} = \xi^2 \in W^2$. Definimos $\varepsilon_1 := \xi^{-1}\varepsilon$. Entonces $\bar{\varepsilon}_1 = \bar{\xi}^{-1}\bar{\varepsilon} = \xi \frac{\varepsilon}{\bar{\varepsilon}} = \xi^{-1}\varepsilon = \varepsilon_1$, esto es, $\varepsilon_1 \in \mathbb{R}$. Por lo tanto $\text{núc } \psi = WE^+$ y tenemos la inyección inducida $E/WE^+ \hookrightarrow W/W^2$ y $|W/W^2| = 2$ puesto que W es cíclico y $2||W|$. Se sigue que $Q = 1$ o 2 . De hecho, si $\phi(E) = W$, entonces $Q = 2$ y si $\phi(E) = W^2$, $Q = 1$. \square

Corolario 13.7.32. Sea $K = \mathbb{Q}(\zeta_n)$ el campo ciclotómico de las n -raíces de la unidad y $n \geq 3$. Entonces $Q = \begin{cases} 1 & \text{si } n = p^m \\ 2 & \text{en otro caso} \end{cases}$.

Demostración. Ver [75, Corolario 4.13, pág. 40]. \square

Teorema 13.7.33. Sea C el grupo de clases de ideales de $\mathbb{Q}(\zeta_n)$, $n \geq 3$ y C^+ el grupo de clases de ideales de $\mathbb{Q}(\zeta_n)^+$. Entonces el mapeo natural $C^+ \rightarrow C$ es inyectivo.

Demostración. Ver [75, Teorema 4.14, pág. 40]. \square

Observación 13.7.34. El Teorema 13.7.33 no se cumple para campos de tipo MC en general. Por ejemplo, si $K = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$, entonces K es de tipo MC y $K^+ = \mathbb{Q}(\sqrt{10})$. El ideal $\mathfrak{p} := \langle 2, \sqrt{10} \rangle$ en $\mathbb{Q}(\sqrt{10})$ no es principal pues si $\langle 2, \sqrt{10} \rangle = \langle \alpha \rangle$ en $\mathbb{Q}(\sqrt{10})$, $N\alpha = N\mathfrak{p} = 2$ pero si $\alpha = a + b\sqrt{10}$, $N\alpha = a^2 - 10b^2 \neq \pm 2$ ya que si fuese posible, $a^2 \equiv \pm 2 \pmod{5} \equiv 2, 3 \pmod{5}$. Sin embargo los residuos módulo 5 son 0, 1, y 4. Por otro lado, sea $C^+ = Cl_{\mathbb{Q}(\sqrt{10})} \xrightarrow{\phi}$

$C = Cl_{\mathbb{Q}(\sqrt{10}, \sqrt{-2})}$ y $\mathfrak{p} = \langle 2, \sqrt{10} \rangle$, $\phi(\mathfrak{p}) = \mathfrak{P}^2$ pues como 2 es ramificado en $\mathbb{Q}(\sqrt{10})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, 2 es totalmente ramificado en K/\mathbb{Q} . Sea $\alpha := -\sqrt{-2} \in K$. Entonces $2 = \alpha(\sqrt{-2})$, $\sqrt{10} = \alpha(-\sqrt{-5})$ por lo que $\mathfrak{p} = \langle \alpha \rangle$ en C y en particular $\bar{\mathfrak{p}} \in \text{nuc } \phi$ y $\bar{\mathfrak{p}} \neq 1$.

Por otro lado se sabe en general que para K de tipo MC, $C^+ \xrightarrow{\phi} C$ satisface que $|\text{nuc } \phi| = 1$ o 2.

Sea K_∞/K una extensión \mathbb{Z}_p tal que K_n es de tipo MC para toda n . Entonces K_∞^+/K^+ es una extensión \mathbb{Z}_p . Notemos que $r_2 = 0$ para K^+ y por tanto K_∞^+/K^+ será la extensión \mathbb{Z}_p -ciclotómica en caso de que la Conjetura de Leopoldt (Conjetura 13.5.9) se cumpla y por lo tanto, en este caso, K_∞/K es la extensión \mathbb{Z}_p -ciclotómica pues $K_\infty = KK_\infty^+ = KK^+\mathbb{Q}_\infty = K\mathbb{Q}_\infty$.

En general, si K es de tipo MC, se tiene que $J \in \text{Gal}(K/K^+)$, $J \neq \text{Id}$ y en particular J es un automorfismo de K . Se tiene que J actúa en varios grupos y módulos asociados a K . Por ejemplo, J actúa en $Cl(K)$ o en $A := Cl(K)(p)$. Si A es un grupo abeliano tal que J actúa en A , definimos

$$A^+ := \{a \in A \mid J(a) = a\} \quad \text{y} \quad A^- := \{a \in A \mid J(a) = -a\}.$$

Si 2 es una unidad en A , lo cual, en el caso finito, significa que 2 no divide al orden de A , se tiene que

$$A = A^+ + A^- \quad \text{y} \quad A^+ \cap A^- = \{0\}.$$

En efecto, si $x \in A$, $x = \frac{x+\bar{x}}{2} + \frac{x-\bar{x}}{2} = y + z$, donde $y = \frac{x+\bar{x}}{2}$, $z = \frac{x-\bar{x}}{2}$. Ahora bien, $\bar{y} = \frac{\bar{x}+\bar{\bar{x}}}{2} = \frac{x+\bar{x}}{2} = y$ y $\bar{z} = \frac{\bar{x}-\bar{\bar{x}}}{2} = -\frac{x-\bar{x}}{2} = -z$, es decir, $y \in A^+$ y $z \in A^-$ lo cual implica que $A^+ + A^- = A$.

Ahora bien, si $x \in A^+ \cap A^-$, entonces $\bar{x} = x = -x$, es decir, $2x = 0$ lo cual implica $x = 0$ pues 2 es unidad en A . Por lo tanto $A^+ \cap A^- = \{0\}$. En consecuencia tenemos $A = A^+ \oplus A^-$.

Por ejemplo, si p es un número primo, $p > 2$ y A es el p -subgrupo de Sylow del grupo de clases de un campo K de tipo MC, tenemos la situación anterior.

Ahora consideremos K_∞/K una extensión \mathbb{Z}_p de tipo MC, $A_n = Cl(K_n)(p)$ con $p > 2$. Entonces $A_n = A_n^+ \oplus A_n^-$, $X_n = X_n^+ \oplus X_n^-$.

$$\begin{array}{ccc}
 & & L_n \\
 & \nearrow^{X_n} & \\
 K_0 & \text{---} & K_n \\
 \downarrow & & \downarrow \{1, J\} \\
 K_0^+ & \text{---} & K_n^+
 \end{array}$$

Puesto que la acción de γ_0 en $\Gamma = \text{Gal}(K_\infty/K)$ conmuta con la acción de J , se tiene que $X = X^+ \oplus X^-$ con $X^+ := \varprojlim_n X_n^+$ y $X^- := \varprojlim_n X_n^-$. Obtenemos como antes $A_n^\pm \cong X_n^\pm \cong \frac{X^\pm}{\gamma_n, eY_n^\pm}$. Además tenemos que $h_n^+ | h_n$ y si definimos $h_n^- := \frac{h_n}{h_n^+}$, se tiene que si $p^{e_n^\pm}$ es la potencia exacta de p que divide a h_n^\pm , entonces

$$\begin{aligned} e_n &= e_n^+ + e_n^- \quad y \quad e_n^\pm = \mu^\pm + \lambda^\pm n + \gamma^\pm \quad \text{con} \\ \mu &= \mu^+ + \mu^-, \quad \lambda = \lambda^+ + \lambda^- \quad y \quad \gamma = \gamma^+ + \gamma^-. \end{aligned}$$

Como obtuvimos antes, se sigue que $\mu^\pm = 0 \iff$ el p -rango de A_n^\pm está acotado.

En el caso $p = 2$, si $x \in A^+ \cap A^-$, entonces $\bar{x} = x = -x$, esto es $2x = 0$, pero no podemos concluir que $x = 0$ y por ende que $A^+ \cap A^- = \{0\}$. Por ejemplo, se tiene que $h(\mathbb{Q}(\sqrt{-5})) = 2$, esto es, $A \cong \mathbb{Z}/2\mathbb{Z}$. Se tiene que $\{I, J\} = \text{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$ y $A^+ = A^- = A$.

Si X es un clase de ideales de K^+ con $X^2 = (1)$, entonces $X \in A^+ \cap A^-$ pues $\bar{X} = X = X^{-1}$.

Sean $p = 2$ y K un campo de clase MC. Definimos $A = \text{Cl}(K)(2)$, $A^- = \{a \in A \mid \bar{a} = a^{-1}\}$ y $A^+ = \text{Cl}(K^+)(2)$. Sea $N: A \rightarrow A^+$, $N = 1 + J$ la norma de K en K^+ pues $\text{Gal}(K/K^+) = \{1, J\}$.

Usando el mapeo de Reciprocidad de Artin, tenemos el diagrama conmutativo

$$\begin{array}{ccc} \text{Cl}(K) = I_K/P_K & \xrightarrow[\text{Artin}]{\cong} & \text{Gal}(H_K/K) \\ \downarrow \text{Norma} & & \downarrow \text{rest} \\ \text{Cl}(K^+) = I_{K^+}/P_{K^+} & \xrightarrow[\text{Artin}]{\cong} & \text{Gal}(H_{K^+}/K^+) \end{array}$$

donde H_K y H_{K^+} denotan los campos de clase de Hilbert de K y K^+ respectivamente.

Puesto que $K \cap H_{K^+} = K^+$ debido a que los primos arquimideanos son ramificados el mapeo de restricción rest es suprayectivo de donde se sigue que el mapeo norma $N: \text{Cl}(K) = I_K/P_K \rightarrow \text{Cl}(K^+) = I_{K^+}/P_{K^+}$ es sobre.

$$\begin{array}{ccc} & & H_K \\ & & \downarrow \\ H_{K^+} & \xrightarrow{\quad} & H_{K^+}K \\ \downarrow \text{||} & & \downarrow \text{||} \\ K^+ & \xrightarrow{\quad} & K \end{array}$$

Por tanto $N: A \rightarrow A^+$ es suprayectivo y

$$\text{núc } N = \{a \mid (1+J)a = a^{1+J} = a\bar{a} = 1\} = \{a \in A \mid \bar{a} = a^{-1}\} = A^-$$

por lo que tenemos la sucesión exacta

$$0 \longrightarrow A^- \longrightarrow A \longrightarrow A^+ = Cl(K^+)(2) \longrightarrow 0.$$

Como antes se sigue que $\mu = \mu^+ + \mu^-$, $\lambda = \lambda^+ + \lambda^-$, $\gamma = \gamma^+ + \gamma^-$, $\mu^+ = 0$ si y solamente si el 2-rango de $Cl(K_n^+)(2)$ está acotado y $\mu^- = 0$ si y solamente si el 2-rango de A_n^- está acotado.

Ahora bien, cuando $p > 2$, se tiene que si $A = Cl(K)(p)$, $A^+ = \{a \in A \mid a^J = a\}$, entonces $A^+ \cong Cl(K^+)(p)$. Más generalmente, tenemos:

Proposición 13.7.35. *Sea F un campo numérico finito y sea K una extensión de Galois de F de grado d . Sea ℓ un número primo que no divide a d . El homomorfismo natural $Cl_F(\ell) \rightarrow Cl_K(\ell)$ es inyectivo, la norma $N_{K/F}: Cl_K(\ell) \rightarrow Cl_F(\ell)$ es suprayectivo y las siguientes condiciones son equivalentes*

- (I) $Cl_F(\ell) = Cl_K(\ell)$.
- (II) ℓ -rango de $Cl_F(\ell) = \ell$ -rango de $Cl_K(\ell)$.
- (III) La norma $N_{K/F}: Cl_K(\ell) \rightarrow Cl_F(\ell)$ es un isomorfismo.

Demostración. Sea $N = N_{K/F}$. Sea $\mathfrak{a} \in Cl_F(\ell)$ el cual es principal en Cl_K : $\mathfrak{a} = \langle \alpha \rangle$, $\alpha \in K$. Tomando la norma $N\mathfrak{a} = \mathfrak{a}^d = \langle N\alpha \rangle = \langle \beta \rangle$, $\beta \in F$ principal. Por otro lado, existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^{\ell^n} = \langle \gamma \rangle$ con $\gamma \in F$ pues $\mathfrak{a} \in Cl_F(\ell)$. Puesto que $\text{mcd}(d, \ell^n) = 1$, existen $a, b \in \mathbb{Z}$ tales que $1 = ad + b\ell^n$ y $\mathfrak{a} = \mathfrak{a}^{da}\mathfrak{a}^{\ell^{nb}} = \langle \beta^a \gamma^b \rangle$ con $\beta^a \gamma^b \in F$ por lo que \mathfrak{a} es principal y $Cl_F(\ell) \rightarrow Cl_K(\ell)$ es 1-1.

Se tiene que $Cl_F(\ell) \supseteq NCl_K(\ell) \supseteq NCl_F(\ell) = Cl_F(\ell)^d = Cl_F(\ell)$ esta igualdad debido a que d y ℓ son primos relativos. Se sigue que la norma es suprayectiva.

Probemos ahora la última parte.

(I) \Rightarrow (II). Es inmediato

(II) \Rightarrow (III). Puesto que el ℓ -rango de $Cl_F(\ell) = \ell$ -rango de $Cl_K(\ell)$, tenemos que $\frac{Cl_K(\ell)}{\ell Cl_K(\ell)} = \frac{Cl_F(\ell)}{\ell Cl_F(\ell)}$.

Se tiene para un ℓ -grupo abeliano finito A que $|\{x \in A \mid x^\ell = 1\}| = |A/A^\ell|$ de donde obtenemos que si $\mathfrak{a} \in Cl_K(\ell)$ con $\mathfrak{a} \in \text{núc } N$ y $o(\mathfrak{a}) = \ell^n$ para $n \geq 1$, entonces $o(\mathfrak{a}^{\ell^{n-1}}) = \ell$ y $\mathfrak{a}^{\ell^{n-1}} \in \text{núc } N$. Puesto que $|\frac{Cl_K(\ell)}{\ell Cl_K(\ell)}| = |\frac{Cl_F(\ell)}{\ell Cl_F(\ell)}|$, se tiene que $\{x \in Cl_K(\ell) \mid x^\ell = 1\} = \{x \in Cl_F(\ell) \mid x^\ell = 1\}$.

Puesto que $\mathfrak{a}^{\ell^{n-1}} \in \{x \in Cl_K(\ell) \mid x^\ell = 1\}$, $\mathfrak{a}^{\ell^{n-1}} \in Cl_F(\ell)$. Por otro lado $1 = N\mathfrak{a}^{\ell^{n-1}} = \mathfrak{a}^{\ell^{n-1}d}$ lo cual contradice que $o(\mathfrak{a}^{\ell^{n-1}}) = o(\mathfrak{a}^{\ell^{n-1}d}) = \ell$. Por tanto N es 1-1 y puesto que es sobre, N es un isomorfismo.

(III) \Rightarrow (I). Como la conorma es 1-1, podemos poner $Cl_F(\ell) \subseteq Cl_K(\ell)$ y puesto que la norma es un isomorfismo, ambos grupos son del mismo orden de donde se sigue la igualdad $Cl_F(\ell) = Cl_K(\ell)$. \square

En particular obtenemos

Proposición 13.7.36. *Sea K un campo de tipo MC y sea p un número primo. Sea $\mathcal{C}l_K(p)$ el p -subgrupo de Sylow del grupo de clases de ideales $\mathcal{C}l_K$ de K . Entonces*

- (I) *El mapeo natural $\mathcal{C}l_{K^+}(p) \rightarrow \mathcal{C}l_K(p)$ es 1-1 si $p > 2$ y tiene núcleo de orden 1 o 2 si $p = 2$.*
- (II) *La norma $N = N_{K/K^+} : \mathcal{C}l_K(p) \rightarrow \mathcal{C}l_{K^+}(p)$ es suprayectiva.*

Demostración.

(I) Se tiene $[K : K^+] = 2$, por lo que si $p > 2$, $\mathcal{C}l_{K^+}(p) \rightarrow \mathcal{C}l_K(p)$ es inyectiva por la Proposición 13.7.35.

Sea $p = 2$ y sea \mathfrak{a} un ideal en K^+ tal que \mathfrak{a} es principal en K : $\mathfrak{a} = \langle \alpha \rangle$, $\alpha \in K$. Entonces $\bar{\mathfrak{a}} = \langle \bar{\alpha} \rangle = \mathfrak{a} = \langle \alpha \rangle$, por lo que $\frac{\alpha}{\bar{\alpha}}$ es una unidad en \mathcal{O}_K .

Si σ es un encaje de K en \mathbb{C} , entonces, como K es de tipo MC, se tiene $\sigma\left(\frac{\alpha}{\bar{\alpha}}\right) = \frac{\sigma\alpha}{\sigma\bar{\alpha}} = \frac{\sigma(\alpha)}{\overline{\sigma(\alpha)}}$, esto es, $\left|\frac{\sigma\alpha}{\sigma\bar{\alpha}}\right| = 1$ de donde se sigue que $\frac{\alpha}{\bar{\alpha}}$ es una raíz de unidad.

Si en K tenemos $\mathfrak{a} = \langle \beta \rangle$, esto es, $\langle \alpha \rangle = \langle \beta \rangle$, entonces existe $u \in E_K$, unidades de K , tal que $\alpha = \beta u$. Por lo tanto $\frac{\alpha}{\bar{\alpha}} = \frac{\beta}{\bar{\beta}} = \frac{u}{\bar{u}}$. Sea $\varphi : E_K \rightarrow W_K = \text{raíces de unidad en } K$, $u \mapsto \frac{u}{\bar{u}}$. Entonces se tiene $\frac{\alpha}{\bar{\alpha}} = \frac{\beta}{\bar{\beta}} \pmod{\varphi(E_K)}$.
Sea

$$\begin{aligned} \phi : \text{núc}(\mathcal{C}l_{K^+} \rightarrow \mathcal{C}l_K) &\longrightarrow W/\varphi(E_K) \\ \mathfrak{a} &\longmapsto \left[\frac{\alpha}{\bar{\alpha}} \right]. \end{aligned}$$

Veamos que ϕ es inyectiva. De hecho, si $\phi(\mathfrak{a}) = \left[\frac{\alpha}{\bar{\alpha}} \right] = [1]$, entonces

$\frac{\alpha}{\bar{\alpha}} = \frac{u}{\bar{u}}$ con $u \in E_K$ y por lo tanto $\frac{\alpha}{u} = \frac{\bar{\alpha}}{\bar{u}} = \overline{\left(\frac{\alpha}{u}\right)}$, esto es $\frac{\alpha}{u} \in K^+$ y $\mathfrak{a} = \langle \alpha \rangle = \langle \alpha/u \rangle$ por tanto $\bar{\mathfrak{a}} = (1)$. Así ϕ es 1-1. Se sigue que $|\text{núc}(\mathcal{C}l_{K^+} \rightarrow \mathcal{C}l_K)| \leq |W_K/\varphi(E_K)| \leq [W_K : W_K^2] = 2$ pues $W_K/\varphi(E_K)$ se puede encajar en W_K/W_K^2 el cual es de orden 2 debido a que W_K es cíclico de orden par.

(II) Si H_K y H_{K^+} son los campos de clase de Hilbert, entonces tenemos el diagrama conmutativo:

$$\begin{array}{ccc} \mathcal{C}l_K = I_K/P_K & \xrightarrow[\text{Artin}]{\cong} & \text{Gal}(H_K/K) \\ N \downarrow & & \downarrow \text{rest} \\ \mathcal{C}l_{K^+} = I_{K^+}/P_{K^+} & \xrightarrow[\text{Artin}]{\cong} & \text{Gal}(H_{K^+}/K^+) \end{array}$$

de donde se sigue que N es suprayectiva. \square

Proposición 13.7.37. *Si p es un número primo, $p > 2$, y K es un campo numérico finito de tipo MC, entonces si $A = Cl_K(p)$, se tiene $A^+ \cong Cl_{K^+}(p)$.*

Demostración. Se tiene que $A^+ = \{a \in A \mid \bar{a} = a\} = \{a \in A \mid a^{J-1} = 1\}$. Sea $N: Cl_K(p) \rightarrow Cl_{K^+}(p)$, $N = 1 + J$. Entonces N es suprayectivo (Proposición 13.7.36) y

$$\begin{aligned} \text{núc } N &= \{x \in Cl_K(p) \mid Nx = x^{J+1} = \bar{x}x = 1\} = \\ &= \{x \in Cl_K(p) \mid \bar{x} = x^{-1}\} = A^-. \end{aligned}$$

Por tanto tenemos la sucesión exacta

$$0 \longrightarrow A^- \longrightarrow A \longrightarrow Cl_{K^+}(p) \longrightarrow 0.$$

Por otro lado, puesto que $A = A^+ \oplus A^-$ se tiene

$$A^+ \cong A/A^- \cong Cl_{K^+}(p). \quad \square$$

Resumiendo los resultados anteriores, tenemos: para $A = Cl_K(p)$ donde K es un campo numérico finito de clase MC, se tiene

$$A^- = \{x \in A \mid \bar{x} = x^{-1}\} \quad \text{y} \quad A^+ = \begin{cases} \{x \in A \mid \bar{x} = x\} \cong Cl_{K^+}(p) & \text{si } p > 2 \\ Cl_{K^+}(2) & \text{si } p = 2 \end{cases}.$$

Si $p > 2$, $A \cong A^+ \oplus A^-$ y si $p = 2$, entonces se tiene la sucesión exacta $1 \longrightarrow A^- \longrightarrow A \longrightarrow A^+ \longrightarrow 1$.

Teorema 13.7.38. *Sean K un campo numérico finito de MC, p un número primo impar. Supongamos que $\zeta_p \in K$. Sea $A = Cl_K(p)$. Entonces $\text{rango}_p A^+ \leq \text{rango}_p A^- + 1$.*

Sea W_K el grupo de las raíces de unidad en K . Si $K(W_K^{1/p})/K$ es ramificada, entonces $\text{rango}_p A^+ \leq \text{rango}_p A^-$.

Demostración. Se L la máxima extensión abeliana no ramificada de K de exponente p y sea $G := \text{Gal}(L/K)$. Entonces, por teoría de campos de clase, $G \cong Cl_K/Cl_K^p \cong {}_p Cl_K$ y sea $G^+ := Cl_{K^+}/Cl_{K^+}^p \cong {}_p Cl_{K^+}$.

Puesto que $\zeta_p \in K$, L/K es una extensión de Kummer. Sea B el grupo $(K^*)^p \subseteq B \subseteq K^*$ tal que $L = K(B^{1/p})$. Se tiene el mapeo de Kummer

$$\begin{array}{ccc} & L & \\ \mathcal{G} \swarrow & & \downarrow G \\ K^+ & \xrightarrow{\{1, J\}} & K \end{array} \quad \begin{aligned} G \times B/(K^*)^p &\longrightarrow {}_p W_K = \{\xi \in \mathbb{C}^* \mid \xi^p = 1\} \\ (\sigma, \bar{b}) &\longmapsto \frac{\sigma(b^{1/p})}{b^{1/p}}. \end{aligned}$$

Se tiene que L es Galois sobre K^+ y si $\mathcal{G} = \text{Gal}(L/K^+)$, entonces $1 \rightarrow G \rightarrow \mathcal{G} \rightarrow \{1, J\} \rightarrow 1$ es exacta. Es decir, $\{1, J\}$ actúa en G por medio de conjugación. Puesto que p es impar, se tiene $G \cong G^+ \times G^-$.

Sea $V := B/(K^*)^p$. Entonces J actúa en V y nuevamente tenemos que $V \cong V^+ \times V^-$. Sea $\sigma \in G^+$, esto es, $J \circ \sigma = \sigma$, es decir, $\overline{\sigma(b^{1/p})} = \sigma(b^{1/p})$. Ahora bien, consideremos $R := \{[b] \in V \mid (\sigma, [b]) = 1 \ \forall \ \sigma \in G^+\}$. Entonces $\bar{b} \in R \iff \frac{\sigma(b^{1/p})}{b^{1/p}} = 1$ para toda $\sigma \in G^+ \iff \sigma(b^{1/p}) = b^{1/p} \ \forall \ \sigma \in G^+ \iff b^{1/p} = \sigma(b^{1/p}) = \overline{\sigma(b^{1/p})} = \bar{b}^{1/p}$.

Se sigue que $R = V^+$ y por tanto $G^+ \times V/V^+ \cong G^+ \times V^- \rightarrow {}_pW_K$ es un mapeo bilineal no degenerado. Se sigue que $G^+ \cong V^-$.

En particular $\text{rango}_p G^+ = \text{rango}_p A^+ = \text{rango}_p V^-$. Se tiene que si $b \in B$, puesto que $L = K(B^{1/p})$ y L/K es no ramificada, entonces $K(b^{1/p})/K$ es no ramificada.

Sea $\mathfrak{a} := \langle b^{1/p} \rangle$ en $K(b^{1/p})$, esto es, $\mathfrak{a}^p = \langle b \rangle$. Sea $\langle b \rangle = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_r^{s_r}$ con $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ divisores primos de K y sean $\mathfrak{p}_i = \mathfrak{P}_{i1} \cdots \mathfrak{P}_{ir}$. Entonces como $K(b^{1/p})/K$ es no ramificada, $p|s_1, \dots, p|s_r$ y $\langle b \rangle = \mathfrak{B}^p$ para un ideal \mathfrak{B} de K .

El mapeo $\begin{matrix} B & \longrightarrow & \mathcal{C}l_K \\ b & \longmapsto & \overline{\mathfrak{B}} \end{matrix}$ se puede levantar a un homomorfismo a $V: V = B/K^{*p} \xrightarrow{\varphi} {}_p\mathcal{C}l_K = \{x \in \mathcal{C}l_K \mid x^p = 1\}$ el cual induce a su vez un homomorfismo $\varphi^-: V^- \rightarrow {}_p\mathcal{C}l_K^-$ ya que $\varphi \circ J = J \circ \varphi$. Ahora bien probaremos que existe un mapeo inyectivo núc $\varphi^- \rightarrow (E_K/E_K^p)^-$. Sea $b \in \text{núc } \varphi^-$, $\mathfrak{B}^p = \langle b \rangle$, $\varphi(b) = \overline{\mathfrak{B}} = \langle 1 \rangle$, es decir, $\mathfrak{B} = \langle a \rangle$ por lo que $\langle a^p \rangle = \langle b \rangle$. Entonces existe $u \in E_K$ tal que $b = a^p u$. Puesto que $b \in V^-$, $a^{-p} u^{-1} = b^{-1} = \bar{b} = \overline{a^p u} = \overline{a^p} \bar{u}$. Por tanto $\bar{u} = u^{-1}$ por lo que $u \in E_K^-$. Entonces se tiene el mapeo núc $\varphi^- \rightarrow (E_K/E_K^p)^-$, $b \mapsto u$.

Se tiene $[E_K : E_{K^+} W_K] = 1$ o 2 , lo cual implica que $\frac{E_K}{E_K^p} \cong \frac{(E_K W_K)}{(E_K W_K)^p}$ debido a que $p > 2$. De hecho si C y D son grupos abelianos $D < C$ y $[C : D] = 2$ y si p es un número primo, $p > 2$, entonces el mapeo natural $D/D^p \rightarrow C/C^p$ es un isomorfismo; sea $C = C \uplus \xi D$ y $D \xrightarrow{\theta} C$ el encaje natural. Por tanto $\theta(D^p) \subseteq C^p$ y θ induce $D/D^p \xrightarrow{\tilde{\theta}} C/C^p$. Para $x = \xi y$, $y \in D$ entonces $x \equiv x x^{-p} \text{ mód } C^p \equiv \xi y \xi^{-p} y^{-p} = (\xi^2)^{-(p-1)/2} y^{1-p} \in D$ y en particular $\tilde{\theta}((\xi^2)^{-(p-1)/2} y^{1-p}) = x \text{ mód } C^p$ y $\tilde{\theta}$ es un isomorfismo.

Volviendo a nuestra demostración, se tiene la sucesión exacta

$$1 \longrightarrow \frac{W_K}{W_K^p} \longrightarrow \frac{E_{K^+} W_K}{(E_{K^+} W_K)^p} \longrightarrow \text{subgrupo de } \left(\frac{E_{K^+}}{E_{K^+}^p} \right) \longrightarrow 1.$$

Puesto que $p > 2$ y $\left(\frac{E_{K^+}}{E_{K^+}^p} \right)^+ = \frac{E_{K^+}}{E_{K^+}^p}$ tomando la parte $(-)$ en la sucesión exacta se tiene que

$$\mathbb{Z}/p\mathbb{Z} \cong \frac{W_K}{W_K^p} \cong \left(\frac{W_K}{W_K^p} \right)^- = \left(\frac{E_{K^+} W_K}{(E_{K^+} W_K)^p} \right)^-.$$

Por lo tanto $G^+ \cong V^-$, $V^- \xrightarrow{\varphi^-} {}_p\mathcal{C}l_K^{-1}$ y

$$\text{rango}_p(\text{núc } \varphi^-) \leq \text{rango}_p(E_K/E_K^p)^- = 1.$$

Resumiendo

$$\begin{aligned} \text{rango}_p A^+ &= \text{rango}_p G^+ = \text{rango}_p V^- \leq \\ &\leq \text{rango}_p A^- + \text{rango}_p \text{núc } \varphi^- = \text{rango}_p A^- + 1. \end{aligned}$$

Finalmente, si $K(W_K^{1/p})$ es ramificada, entonces B no contiene a W_K y por lo tanto

$$\begin{aligned} \text{núc } \varphi^- &\xrightarrow{\lambda} (E_K/E_K^p)^- = (W_K/W_K^p)^- = \mathbb{Z}/p\mathbb{Z} \\ b &\longmapsto u \end{aligned}$$

por lo que si $b \in \text{núc } \varphi^-$, entonces $u = 1$ y $b = 1$, esto es, λ no puede ser suprayectiva de donde $\lambda = 1$, $\text{núc } \varphi^- = \{1\}$ y $\text{rango}_p A^+ \leq \text{rango}_p A^-$. \square

Corolario 13.7.39. Sean $p > 0$ y $K = \mathbb{Q}(\zeta_p)$. Sea h_p el número de clase de K . Se tiene que si $p \nmid h_p^-$ entonces $p \nmid h_p^+$ y consecuentemente $p \nmid h_p$.

Demostración. Se tiene que $W_K = \langle \zeta_{2p} \rangle$ y $W_K^{1/p} = \langle \zeta_{2p^2} \rangle$, $K(W_K^{1/p}) = \mathbb{Q}(\zeta_{2p^2}) = \mathbb{Q}(\zeta_{p^2})$, esto es, $K(W_K^{1/p})/K$ es ramificada por lo que $\text{rango}_p A^+ \leq \text{rango}_p A$ donde $A = \mathcal{C}l(K)$. Por hipótesis, tenemos que $\text{rango}_p A^- = 0$ pues $p \nmid h_p^-$ lo cual implica que $\text{rango}_p A^+ = 0$ y por ende $p \nmid h_p^+$. \square

Observación 13.7.40. Se tiene que si $p = 37$, $h_{37}^- = 37$ por lo que $37|h_{37}^-$.

Similarmente, se tiene que $h_{69}^- = 69$ aunque en este caso 69 no es primo.

Para $p = 2$, se tiene:

Teorema 13.7.41. Sea K un campo numérico finito de tipo MC y sean A_K , A_{K^+} los 2-subgrupos de Sylow de los grupos de clases de K y K^+ respectivamente. Entonces

$$\text{rango}_2 A_{K^+} \leq 1 + \text{rango}_2 A_K^-.$$

Demostración. Sea $\varphi: A_{K^+} \rightarrow A_K$ el mapeo natural. Se tiene que $|\text{núc } \varphi| = 1$ o 2. Ahora si $x \in {}_2\varphi(A_{K^+}) = \{x \in \varphi(A_{K^+}) \mid x^2 = 1\}$, entonces $x \in {}_2A_K^- = \{x \in A_K^- \mid x^2 = 1\}$ pues si $x^2 = 1$, se tiene $x = x^{-1}$ y puesto que $x \in \varphi(A_{K^+})$, $\bar{x} = x$ lo cual implica que $\bar{x} = x = x^{-1}$, es decir, $x \in A_K^-$.

De esta forma obtenemos $\text{rango}_2 {}_2\varphi(A_{K^+}) \leq \text{rango}_2 {}_2A_K^-$. Por lo tanto

$$|\text{núc } \varphi| = \frac{|{}_2A_{K^+}|}{|{}_2\varphi(A_{K^+})|} = 1 \text{ o } 2, \text{ por tanto } \text{rango}_2 \varphi(A_{K^+}) \geq \text{rango}_2 A_{K^+} - 1.$$

Finalmente obtenemos

$$\text{rango}_2 A_{K^+} \leq \text{rango}_2 \varphi(A_{K^+}) + 1 \leq \text{rango}_2 A_K^- + 1. \quad \square$$

Sea ahora K_∞/K una extensión \mathbb{Z}_p tal que K_n es de tipo MC. Se tiene $\mu = \mu^+ + \mu^-$ y $\mu = 0$ si y solamente si $\text{rango}_p A_n$ está acotado.

Corolario 13.7.42. *Se tiene que si $\mu^- = 0$, entonces $\mu^+ = 0$ y por ende $\mu = 0$. En consecuencia, para cualquier número primo p , $\mu = 0 \iff \mu^- = 0$.*

Demostración. Si $\mu^- = 0$, el p -rango de A_n^- está acotado y por lo tanto el p -rango de A_n^- está acotado. Se sigue que $\mu^+ = 0$ y $\mu = \mu^+ + \mu^- = 0 + 0 = 0$. \square

Proposición 13.7.43. *Sea K_∞/K una extensión \mathbb{Z}_p tal que $\mu = 0$. Entonces si L es la máxima p -extensión abeliana de K_∞ no ramificada, se tiene*

$$X := \text{Gal}(L/K_\infty) \cong \varprojlim_n A_n \cong \mathbb{Z}_p^\lambda \oplus (p\text{-grupo finito}).$$

Demostración. Se tiene que $X \sim E = \bigoplus_{j=1}^s \Lambda / \langle f_j(T)^{m_j} \rangle$, $\lambda = \sum_{j=1}^s m_j \text{gr } f_j(T)$.

Por el algoritmo de la división, obtenemos que $E \cong \mathbb{Z}_p^\lambda$ como \mathbb{Z}_p -módulo. Puesto que X es \mathbb{Z}_p -módulo finitamente generado pues E lo es, por el teorema sobre la estructura de módulos sobre un dominio de ideales principales (pues \mathbb{Z}_p lo es) se sigue que el \mathbb{Z}_p -rango de X es λ . \square

Ahora consideremos una situación dual. Sea el mapeo natural $A_n \xrightarrow{\phi_{n,m}} A_m$
 $\bar{\mathfrak{a}} \mapsto \bar{\mathfrak{a}}$
para $m \geq n$. Se tiene

$$\text{Gal}(L_n/K_n) = X_n \cong X / \gamma_{n,e} Y_e \xrightarrow[\text{Artin}]{\cong} A_n \quad \text{para } n \geq e.$$

$$\begin{array}{ccccc} & & & L & \\ & & & \downarrow & \\ & L_n & & & \\ & \downarrow X_n & & & \\ K_0 & \text{---} & K_n & \text{---} & K_\infty \end{array}$$

$$\begin{aligned} A_n &\xrightarrow{\cong} X_n = \text{Gal}(L_n/K_n) \\ C &\mapsto \left(\frac{L_n|K_n}{\mathfrak{a}} \right) \end{aligned}$$

donde $\left(\frac{L_n|K_n}{\mathfrak{a}} \right)$ donde es el símbolo de Artin y $\mathfrak{a} \in C$. Así

$$\begin{aligned} A_n &\xrightarrow{\cong} X/\gamma_{n,e}Y_e \\ C &\mapsto x \text{ mód } \gamma_{n,e}Y_e, \end{aligned}$$

con $x|_{L_n} = \left(\frac{L_n|K_n}{\mathfrak{a}}\right)$ y $\mathfrak{a} \in C$.

Teorema 13.7.44. Para $m \geq n \geq e$, los siguientes diagramas son conmutativos:

$$\begin{array}{ccc} A_n & \xrightarrow[t_n]{\sim} & X/\gamma_{n,e}Y_e \\ \phi_{n,m} \downarrow & & \varepsilon_{n,m} \downarrow \\ A_m & \xrightarrow[t_m]{\sim} & X/\gamma_{m,e}Y_e \end{array} \quad \begin{array}{ccc} A_m & \xrightarrow[t_m]{\sim} & X/\gamma_{m,e}Y_e \\ N_{m,n} \downarrow \text{norma} & & \downarrow \text{rest} \\ A_n & \xrightarrow[t_n]{\sim} & X/\gamma_{n,e}Y_e \end{array}$$

donde

$$\begin{aligned} \varepsilon_{n,m}: X/\gamma_{n,e}Y_e &\longrightarrow X/\gamma_{m,e}Y_e, \quad \varepsilon_{n,m}(x \text{ mód } \gamma_{n,e}Y_e) = \gamma_{m,n}x \text{ mód } \gamma_{m,e}Y_e, \\ \gamma_{m,n} &= \frac{\gamma_m}{\gamma_n} = \frac{(1+T)^{p^m} - 1}{(1+T)^{p^n} - 1} \end{aligned}$$

y t_n, t_m son los mapeos de Artin.

Demostración. El segundo diagrama ya lo conocemos de la teoría de campos de clase.

Sea $x \in X$ y sea \mathfrak{A} un ideal de K_m en A_m tal que $x|_{K_m} = \left(\frac{L_m|K_m}{\mathfrak{A}}\right)$. Para el primer diagrama, si ρ varía sobre todos los elementos de $\text{Gal}(K_m/K_n)$, entonces

$$\begin{aligned} \mathfrak{a} &= N_{m,n}\mathfrak{A} \prod_{\rho \in \text{Gal}(K_m/K_n)} \rho(\mathfrak{A}), \\ (t_m \circ \phi_{n,m})(\bar{\mathfrak{a}}) &= t_m(\bar{\mathfrak{a}}) = \left(\frac{L_m|K_m}{\mathfrak{a}}\right) = \prod_{\rho \in \text{Gal}(K_m/K_n)} \left(\frac{L_m|K_m}{\rho(\mathfrak{A})}\right) \\ &= \prod_{\rho} \rho \circ \left(\frac{L_m|K_m}{\mathfrak{A}}\right) = \prod_{\rho} \rho(x|_{K_m}) = \gamma_{m,n}x|_{K_m} \\ &= (\varepsilon_{n,m} \circ t_n)(\bar{\mathfrak{a}}). \quad \square \end{aligned}$$

Por lo tanto si $A = \varinjlim_n A_n \cong \varinjlim_{\varepsilon_{n,m}} X/\gamma_{n,e}Y_e$, se tiene el diagrama conmutativo de sucesiones exactas

$$\begin{array}{ccccccc} 0 & \longrightarrow & Y_e/\gamma_{n,e}Y_e & \longrightarrow & X/\gamma_{n,e}Y_e & \longrightarrow & X/Y_e \longrightarrow 0 \\ & & \downarrow \varepsilon_{n,m} & & \downarrow \varepsilon_{n,m} & & \downarrow \varepsilon_{n,m} = \gamma_{m,n} \\ 0 & \longrightarrow & Y_e/\gamma_{m,e}Y_e & \longrightarrow & X/\gamma_{m,e}Y_e & \longrightarrow & X/Y_e \longrightarrow 0 \end{array} \quad n \leq m.$$

Para $m \gg n$, $\varepsilon_{n,m} = \gamma_{m,n}: X/Y_e \rightarrow X/Y_e$ es 0 pues $\gamma_{m,e}X \subseteq Y_e$. Es decir, tenemos $A = \varinjlim_n A_n \cong \varinjlim_n Y_e/\gamma_{n,e}Y_e$.

Similarmente si $Y_e \sim E = \left(\bigoplus_{i=1}^t \Lambda/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^s \Lambda/\langle g_j(T) \rangle \right)$, $A \cong \varinjlim_n E/\gamma_{n,e}E$.

Además para $V := \Lambda/\langle p^k \rangle$, $V/\gamma_{n,e}V \cong \{p(T) \bmod \langle p^k, \gamma_{n,e} \rangle \mid p(T) \in \mathbb{Z}_p[T]\} \cong \frac{(\mathbb{Z}/p^k\mathbb{Z})[T]}{T^{p^n-p^e}} \cong C_{p^k}^{p^n-p^e}$ pues $\gamma_{n,e}$ es un polinomio distinguido de grado $p^n - p^e$.

Para $V = \Lambda/\langle g(T) \rangle$ con $g(T)$ polinomio distinguido de grado d , se tiene $\frac{\gamma_{n+2,e}}{\gamma_{n+1,e}} = \frac{P_{n+2}(T)}{P_{n+1}(T)}$ donde $P_n(T) = (1+T)^{p^n} - 1$ y $\frac{P_{n+2}(T)}{P_{n+1}(T)}$ actúa en $\Lambda/\langle g(T) \rangle$, para $p^n \geq d$, como $p \times$ unidad.

De esta forma tenemos:

$$\begin{aligned} 0 \longrightarrow V/pV &\cong \Lambda/\langle p, g(T) \rangle \cong \Lambda/\langle p, T^d \rangle \cong \mathbb{F}_p[T]/\langle T^d \rangle \longrightarrow \\ &\longrightarrow V/\gamma_{n+2,e}V \xrightarrow{\frac{\gamma_{n+2,e}}{\gamma_{n+1,e}}} V/\gamma_{n+1,e}V \longrightarrow 0, \\ V/\gamma_{n,e}V &\cong C_{p^{a_1,n}} \oplus \cdots \oplus C_{p^{a_d,n}} \quad \text{con } a_{i,n+1} = 1 + a_{i,n} \text{ para toda } i. \end{aligned}$$

Por tanto $\varinjlim_n E/\gamma_{n,e}E \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\sum_{j=1}^s \text{gr } g_j} \oplus B$ con $p^a B = 0$ donde $a \geq \max\{k_j \mid 1 \leq i \leq t_i\}$. Además $B = 0 \iff t = 0 \iff \mu = 0$. Se tiene

$$\begin{aligned} \mathbb{Q}_p/\mathbb{Z}_p &=: R \cong W(p) = \{\xi \in \mathbb{C}^* \mid \xi^{p^n} = 1 \text{ para algún } n \in \mathbb{N}\} = \\ &= \bigcup_{n=1}^{\infty} \frac{(1/p^n)\mathbb{Z}}{\mathbb{Z}} = \bigcup_{n=1}^{\infty} \langle \zeta_{p^n} \rangle. \end{aligned}$$

Por tanto tenemos

Teorema 13.7.45. *Si K_∞/K es una extensión \mathbb{Z}_p y si A_n es el p -subgrupo de Sylow de $Cl(K_n)$, se tiene que si $A := \varinjlim_n A_n$, entonces $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \oplus A'$ con A' de exponente acotado, esto es, $p^a A = 0$ para algún $a \in \mathbb{N}$. Además $A' = 0 \iff \mu = 0$ y por tanto A es un grupo divisible $\iff \mu = 0$. \square*

Observación 13.7.46. Lo anterior muestra que puesto que $\mathbb{Q}_p/\mathbb{Z}_p$ es divisible, la conjetura de Iwasawa de que $\mu = 0$ es equivalente a que A sea divisible.

Proposición 13.7.47. *Sean p un primo impar y K un campo numérico finito de tipo MC. Sea K_∞/K la extensión \mathbb{Z}_p -ciclotómica. Entonces el mapeo $A_n^- \rightarrow A_{n+1}^-$ es inyectivo.*

Demostración. Sea I un ideal en K_n que se hace principal K_{n+1} , $\bar{I} \in A_n$. Digamos $I = \langle \alpha \rangle$, $\alpha \in K_{n+1}$. Sea $\langle \sigma \rangle = \text{Gal}(K_{n+1}/K_n)$. Entonces $\langle \alpha^{\sigma^{-1}} \rangle = \frac{I^\sigma}{I} = (1)$, esto es, $\alpha^{\sigma^{-1}} = \varepsilon \in E_{n+1}$, E_{n+1} las unidades de K_{n+1} .

Sea N la norma de K_{n+1}/K_n . Por lo tanto

$$N\varepsilon = N\alpha^{\sigma^{-1}} = \frac{N\alpha^\sigma}{N\alpha} = \frac{N\alpha}{N\alpha} = 1.$$

Por tanto $\tilde{I} \rightarrow \varepsilon$ induce el mapeo

$$\begin{aligned} \text{núc}(A_n \rightarrow A_{n+1}) &\longrightarrow \frac{\text{núc } N|_{E_{n+1}}}{I_{\langle \sigma \rangle} E_{n+1}} = \frac{\text{núc } N|_{E_{n+1}}}{E_{n+1}^{\langle \sigma^{-1} \rangle}} \\ &:= H^{-1}(\text{Gal}(K_{n+1}/K_n), E_{n+1}). \end{aligned}$$

Sea I que representa a una clase en A_n^- . Entonces $\langle \alpha^{1+J} \rangle = I^{1+J} = \langle \beta \rangle$, $\beta \in K_n$, por lo que $\beta^\sigma = \beta$. Se sigue que $\alpha^{1+J} = \beta\eta$ con $\eta \in E_{n+1}$.

Sea $\alpha_1 = \frac{\alpha^2}{\eta}$, $\varepsilon_1 = \alpha_1^{\sigma^{-1}} = \frac{(\alpha^{\sigma^{-1}})^2}{\eta^{\sigma^{-1}}} = \frac{\varepsilon^2}{\eta^{\sigma^{-1}}} \in E_{n+1}$ y

$$\begin{aligned} \varepsilon_1^{1+J} &= (\alpha_1^{1+J})^{\sigma^{-1}} = \left(\left(\frac{\alpha^2}{\eta} \right)^{1+J} \right)^{\sigma^{-1}} = \left(\frac{(\alpha^{1+J})^2}{\eta^{1+J}} \right)^{\sigma^{-1}} = \left(\frac{(\beta\eta)^2}{\eta^{1+J}} \right)^{\sigma^{-1}} \\ &= (\beta^2)^{\sigma^{-1}} (\eta^2 \eta^{-1-J})^{\sigma^{-1}} = 1 \cdot (\eta^{1-J})^{\sigma^{-1}} = (\eta^{\sigma^{-1}})^{1-J} \in E_{n+1}^-. \end{aligned}$$

Además

$$\begin{aligned} E_{n+1}^- &= \{\varepsilon \in E_{n+1} \mid \varepsilon^{1+J} = 1\} = \{\varepsilon \in E_{n+1} \mid \bar{\varepsilon} = \varepsilon^{-1}\} \\ &= \{\varepsilon \in E_{n+1} \mid |\varepsilon| = 1\} \quad \text{y} \quad (\varepsilon^\sigma)^{1+J} = (\varepsilon^{1+J})^\varepsilon = 1^\sigma = 1 \end{aligned}$$

por lo que $E_{n+1}^- = W_{n+1}$ las raíces de unidad en K_{n+1} .

Por lo tanto $(\varepsilon_1^m)^{1+J} = 1$ para alguna m . También $N\varepsilon_1 = (N\alpha_1)^{\sigma^{-1}} = 1$. Se tiene que $H^1(\text{Gal}(K_{n+1}/K_n), W_{n+1}) = \{1\}$, esto es, si $\varepsilon_1 \in W_{n+1}$ y $N\varepsilon_1 = 1$, entonces existe $\varepsilon_2 \in W_{n+1}$ tal que $\varepsilon_1 = \varepsilon_2^{\sigma^{-1}}$.

En efecto, $\varepsilon_1 = \alpha_1^{\sigma^{-1}}$ pero requerimos $y \in W_{n+1}$ tal que $y^{\sigma^{-1}} = \varepsilon_1$. Sean las dos sucesiones exactas

$$\begin{aligned} 1 &\longrightarrow W_n \longrightarrow W_{n+1} \xrightarrow{\sigma^{-1}} W_{n+1}^{\sigma^{-1}} \longrightarrow 1 \\ 1 &\longrightarrow (W_{n+1} \cap \text{núc } N) \longrightarrow W_{n+1} \xrightarrow{N} W_n \longrightarrow 1. \end{aligned}$$

Para verificar la exactitud de la segunda sucesión hay que ver que N es sobre. Si $\zeta_p \notin K_0$, $\zeta_p \notin K_m$ para toda m y en este caso $NW_n = W_n^p = W_n$ y por tanto N es sobre. Ahora, si $\zeta_p \in K_0$, $K_{n+1} = K_n(\zeta_p^m)$ para algún $m \geq n+1$ y $W_{n+1} = \langle \zeta_{p^m} \rangle \times \langle \zeta_t \rangle$ con $\text{mcd}(t, p) = 1$ y $W_n = \langle \zeta_{p^m}^p \rangle \times \langle \zeta_t \rangle$, $N\zeta_{p^m} = \zeta_{p^{m-1}} = \zeta_{p^m}^p$ y $N\zeta_t = \zeta_t^p$ y como $\text{mcd}(t, p) = 1$ se tiene que $\langle \zeta_t \rangle = \langle \zeta_t^p \rangle$ de donde $NW_{n+1} = W_n$.

Así $|W_{n+1}^{\sigma-1}| = \frac{|W_{n+1}|}{|W_n|} = |W_{n+1} \cap \text{núc } N|$ y puesto que $W_{n+1}^{\sigma-1} \subseteq W_{n+1} \cap \text{núc } N$ se sigue la igualdad.

Regresando a nuestra demostración, se tiene que $\alpha_1^{\sigma-1} = \varepsilon_1 = \varepsilon_2^{\sigma-1}$ para alguna $\varepsilon_2 \in W_{n+1}$ por lo tanto $(\frac{\alpha_1}{\varepsilon_2})^\sigma = \frac{\alpha_1}{\varepsilon_2}$ lo cual implica que $\frac{\alpha_1}{\varepsilon_2} \in K_n$.

Sin embargo $\langle \frac{\alpha_1}{\varepsilon_2} \rangle = \langle \alpha_1 \rangle = \langle \alpha^2 \rangle = I^2$ en K_{n+1} lo cual implica $\langle \frac{\alpha_1}{\varepsilon_2} \rangle = I^2$ en K_n por lo que I^2 es principal. Puesto que $p \neq 2$ y $o(\bar{I})$ es una potencia de p , $\bar{I} \in A_n^-$, se sigue que I es principal en K_n y por tanto $A_n^- \rightarrow A_{n+1}^-$ es inyectiva como queríamos probar. \square

Observación 13.7.48. El mapeo $A_n^+ \rightarrow A_{n+1}^+$ no necesariamente es inyectivo y si $p = 2$, entonces el mapeo $A_n^- \rightarrow A_{n+1}^-$ no necesariamente es inyectivo. Finalmente tenemos que si $C_n = \mathcal{Cl}(K_n)$, $C_n \xrightarrow{\phi} C_{n+1}$ es la conorma, entonces se tiene $C_n \xrightarrow{\phi} C_{n+1} \xrightarrow{N} C_n$ por lo que $\text{núc } \phi \subseteq A_n = C_n(p)$.

Proposición 13.7.49. Sean p un primo impar y K un campo número finito de tipo MC. Sea K_∞/K la extensión \mathbb{Z}_p -ciclotómica. Entonces $X^- := \varprojlim_n A_n^-$ no contiene A -submódulos finitos. Por tanto hay una inyección $X^- \hookrightarrow (\bigoplus_{i=1}^t A/\langle p^{k_i} \rangle) \oplus (\bigoplus_{j=1}^s A/\langle g_j(T) \rangle)$ con núcleo finito.

Demostración. Sea $F \subseteq X^-$ un A -submódulo finito. Sea γ_0 un generador topológico de $\text{Gal}(K_\infty/K)$. Puesto que F es finito, existe un número natural n_0 tal que para $n \geq n_0$, $\gamma_0^{p^n}$ actúa trivialmente en F . Supongamos que existe $0 \neq x = (\dots, x_m, x_{m+1}, \dots) \in F \subseteq \varprojlim_n A_n^-$ con $X_{m+1} \rightarrow X_m$ con la norma y $x_m \neq 0$ para $m \geq m_0$.

Sea $m \geq m_0, n_0$. Se tiene, por la Proposición 13.7.47, que $x_m \neq 0$ cuando lo mandamos en A_{m+1}^- . Apliquemos $N = 1 + \gamma_0^{p^m} + \gamma_0^{2p^m} + \dots + \gamma_0^{(p-1)p^m}$ a x . Puesto que $m \geq n_0$, este elemento actúa como multiplicación por p puesto que $\gamma_0^{ip^m} x = x$. También se tiene que $N = N_{K_{m+1}/K_m}$ por lo que $px_{m+1} = x_m \neq 0$ en A_{m+1}^- . Por lo tanto $px \neq 0$. Se sigue que $\begin{matrix} F & \xrightarrow{p} & F \\ x & \mapsto & px \end{matrix}$ es 1-1 en el p -grupo finito lo cual únicamente puede suceder si $F = 0$. \square

Corolario 13.7.50. Sea p un primo impar y sea K un campo numérico finito de tipo MC. Sea K_∞/K la extensión \mathbb{Z}_p -ciclotómica. Si $\mu^- = 0$ se tiene que $X^- = \varprojlim_n A_n^- \cong \mathbb{Z}_p^{\lambda^-}$ como \mathbb{Z}_p -módulos.

Demostración. Se tiene que

$$X^- \hookrightarrow \bigoplus_{j=1}^s A/\langle g_j(T) \rangle \quad \text{y} \quad A/\langle g(T) \rangle \cong \mathbb{Z}_p[T]/\langle T^{\text{gr } g} \rangle \cong \mathbb{Z}_p^{\text{gr } g}.$$

Por la estructura de \mathbb{Z}_p módulos, usando que \mathbb{Z}_p es de ideales principales, se sigue que $X^- \cong \mathbb{Z}_p^{\sum_{j=1}^s \text{gr } g_j} = \mathbb{Z}_p^{\lambda^-}$. \square

Ahora estudiaremos la máxima p -extensión abeliana de K_∞ no ramificada fuera de p . Sea F un campo totalmente real y sea p un número primo impar. Sea $K_0 := F(\zeta_p)$, K_∞/K la extensión \mathbb{Z}_p -ciclotómica, M_∞ la máxima p -extensión abeliana de K_∞ no ramificada fuera de p , $\mathfrak{X}_\infty = \text{Gal}(M_\infty/K_\infty)$ y $G = \text{Gal}(M_\infty/K_0)$. Se tiene la sucesión exacta $1 \rightarrow \mathfrak{X}_\infty \rightarrow G \xrightarrow{\pi} \Gamma \rightarrow 1$. Entonces \mathfrak{X}_∞ es un Γ -módulo por conjugación: si $x \in \Gamma$, sea $g \in G$ tal que $\pi(g) = x$ y $\xi \in \mathfrak{X}_\infty$. Entonces $x \circ \xi := g\xi g^{-1}$. Sea M_n la máxima p -extensión abeliana de K_n no ramificada fuera de p y consideremos $\omega_n := \gamma_0^{p^n} - 1 = (1+T)^{p^n} - 1$. Entonces $\text{Gal}(M_n/K_\infty) = \mathfrak{X}_\infty / \omega_n \mathfrak{X}_\infty$. La demostración de esto es la misma que la de cuando $X_n \cong X/Y_n$, es decir, con el subgrupo conmutador pero sin grupos de inercia (ver Propositiones 13.7.6, y 13.7.10).

Como vimos anteriormente, si $r_2 = r_2(K_0)$, entonces

$$\mathbb{Z}_p^{r_2(K_n)+1+\delta_n} \times (p\text{-grupo finito}) = \mathbb{Z}_p^{r_2 p^n + 1 + \delta_n} \times (p\text{-grupo finito}) \\ \cong \text{Gal}(M_n/K)$$

y donde δ_n es el error en la Conjetura de Leopoldt, esto es,

$$\mathfrak{X}_\infty / \omega_n \mathfrak{X}_\infty \cong \mathbb{Z}_p^{r_2 p^n + \delta_n} \times (p\text{-grupo finito}).$$

Ahora bien, tenemos que $\langle p, \omega_n \rangle \subseteq \langle p, T \rangle$ y $\mathfrak{X}_\infty / \langle p, \omega_n \rangle \mathfrak{X}_\infty \cong \mathbb{F}_p^{r_2 p^n + \delta_n} \times (p\text{-grupo finito})$.

Se sigue del Lema de Nakayama (Proposición 13.7.8) y puesto que \mathfrak{X}_∞ es un Λ -módulo finitamente generado, que $\mathfrak{X}_\infty \sim \Lambda^a \oplus (\Lambda\text{-torsión})$ para alguna $a \geq 0$.

Lema 13.7.51. *La sucesión δ_n está acotada.*

Demostración. Supongamos que $\delta_n > 0$ para alguna n . Sea $\{\varepsilon_1, \dots, \varepsilon_r\}$ una base de las unidades de K_n congruentes con 1: $E_1 := E_1(K_n) = \{\xi \mid \xi \in K_n, \xi \text{ unidad y } \xi \equiv 1 \pmod{\mathfrak{p} \mid \mathfrak{p}}\}$.

Rearreglando, suponemos que $\varepsilon_{\delta_n+1}, \dots, \varepsilon_r$ son independientes y generan \overline{E}_1 sobre \mathbb{Z}_p . Entonces se tiene que existen $a_{ij} \in \mathbb{Z}_p$ tales que $\varepsilon_i = \prod_{j=\delta_n+1}^r \varepsilon_j^{a_{ij}}$, $1 \leq i \leq \delta_n$.

Sea a'_{ij} la n -ésima parcial de a_{ij} . Más precisamente $a_{ij} \equiv a'_{ij} \pmod{p^n}$. Sea $\eta_i := \varepsilon_i \cdot \prod_{j=\delta_n+1}^r \varepsilon_j^{-a'_{ij}} = \prod_{j=\delta_n+1}^r \varepsilon_j^{(a_{ij}-a'_{ij})}$, $1 \leq i \leq \delta_n$.

Se tiene que η_i es una p^n -potencia en $\overline{E}_1 \subseteq \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$ y $\eta_1, \dots, \eta_{\delta_n}$ generan un subgrupo $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$ de $K_n^*/(K_n^*)^{p^n}$ ya que $\eta_i = \varepsilon_i \varepsilon_{\delta_n+1}^{\alpha_0} \cdots \varepsilon_r^{\alpha_r}$, $\alpha_j = a'_{ij}$. Puesto que $\zeta_p \in K_0$, $\zeta_{p^n} \in K_n$ y por Teoría de Kummer, $K_n(\{\eta_i^{1/p^n}\}_{i=1}^{\delta_n})/K_n$ es una extensión abeliana con grupo de Galois isomorfo a $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. También por Teoría de Kummer, puesto que η_i es unidad, la extensión es no ramificada fuera de p . Ahora bien, η_i es una p^n potencia en $U_{1,\mathfrak{p}}$ para toda $\mathfrak{p}|p$ por lo que los campos locales respectivos satisfacen, $K_n(\{\eta_i^{1/p^n}\}_{i=1}^{\delta_n})_{\mathfrak{p}} = (K_n)_{\mathfrak{p}}$, esto es $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$ y por tanto cada $\mathfrak{p}|p$ se descompone totalmente en $K_n(\{\eta_i^{1/p^n}\}_{i=1}^{\delta_n})/K_n$ y en particular no son ramificadas. Todo lo anterior prueba que $K(\{\eta_i^{1/p^n}\}_{i=1}^{\delta_n})/K_n$ es no ramificada y en particular $S := K_n(\{\eta_i^{1/p^n}\}_{i=1}^{\delta_n}) \subseteq L_n$ donde L_n es la máxima p -extensión abeliana de K_n no ramificada.

$$\begin{array}{ccc} & S & \text{---} L_n \\ & \nearrow & \nearrow \\ (\mathbb{Z}/p^n\mathbb{Z})^{\delta_n} & & \\ & \nwarrow & \nwarrow \\ & K_n & \end{array} \quad \begin{array}{c} \\ \\ X_n \end{array}$$

En particular, X_n tiene un cociente isomorfo a $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. Para $n \gg 0$ los términos $\Lambda/\langle p^k \rangle$ de $X \sim \left(\bigoplus_{i=1}^t \Lambda/\langle p^{k_i} \rangle \right) \oplus \left(\bigoplus_{j=1}^s \Lambda/\langle g_j(T) \rangle \right)$ no pueden contribuir a $\mathbb{Z}/p^n\mathbb{Z}$ pues son de exponente acotado. Los términos $\bigoplus_{j=1}^s \Lambda/\langle g_j(T) \rangle$ a lo más contribuyen con $\lambda = \sum_{j=1}^s \text{gr } g_j$ de estos términos y en particular $\delta_n \leq \lambda$. \square

Lema 13.7.52. *El Lema 13.7.51 sigue siendo válido en el caso en que $\zeta_p \notin K_0$.*

Demostración. Sea $K'_0 := K_0(\zeta_p)$ y $\delta'_n = \delta(K_n(\zeta_p))$. Se tiene que $\delta_n \leq \delta'_n \leq \lambda_{K_0(\zeta_p)}$. \square

Notemos que $\text{rango}_{\mathbb{Z}_p} \mathfrak{X}_{\infty}/\omega_n \mathfrak{X}_{\infty} = r_2 p^n + \delta_n$, $0 \leq \delta_n \leq \lambda$, lo cual implica:

Teorema 13.7.53. *El módulo \mathfrak{X}_{∞} satisface que $\mathfrak{X}_{\infty} \sim \Lambda^{r_2} \oplus (\Lambda\text{-torsión})$.*

Demostración. La torsión de \mathfrak{X}_{∞} contribuye de la siguiente manera:

- (1) Si $V = \Lambda/\langle p^k \rangle$, entonces $V/\omega_n V = \Lambda/\langle p^k, \omega_n \rangle \Lambda$ y $|V/\omega_n V| = p^{kp^n} < \infty$.
- (2) Si $V = \Lambda/\langle g(T) \rangle$ donde $g(T)$ es un polinomio distinguido de grado d , entonces $|V/\omega_n V| = p^{nd+c}$ donde c es una constante.

De (1) y (2) se sigue que la torsión de \mathfrak{X}_∞ contribuye con submódulos finitos de $\mathfrak{X}_\infty/\omega_n\mathfrak{X}_\infty$ y se tiene que el \mathbb{Z}_p -rango de $\mathfrak{X}_\infty/\omega_n\mathfrak{X}_\infty$ es igual a $r_2p^n + \delta_n = r_2p^n + o(1)$.

Finalmente, $\Lambda/\omega_n\Lambda \cong \mathbb{Z}_p^{r_2}$, lo cual implica que $\mathfrak{X}_\infty \sim \Lambda^{r_2} \oplus (\Lambda\text{-torsión})$. \square

Ahora estudiaremos una relación entre invariantes y los ℓ -subgrupos de Sylow de los niveles K_n en una extensión \mathbb{Z}_p .

Recordemos que si K/F es una extensión de Galois de grado d y ℓ es un primo con $\ell \nmid d$, entonces si $C_F := {}_\ell Cl(F)$ y $C_K = {}_\ell Cl(K)$ son las ℓ partes primarias de los grupos de clases de ideales de F y K respectivamente, entonces la conorma $C_F \hookrightarrow C_K$ es 1-1 y la norma $C_K \xrightarrow{N} C_F$ es suprayectiva y $Cl(F)(\ell) = Cl(K)(\ell)$ si y solamente si $\text{rango}_\ell C_F = \text{rango}_\ell C_K$ lo cual también es equivalente a que la norma $N_{K/F}: Cl(K)(\ell) \rightarrow Cl(F)(\ell)$ es un isomorfismo (Proposición 13.7.35).

Proposición 13.7.54. *Sea p un número primo distinto a ℓ y sea K_n una extensión cíclica de un campo numérico K_0 de grado p^n . Sean $f = o(\ell \bmod p^n)$ y C_γ la parte ℓ -primaria, es decir, el ℓ -subgrupo de Sylow del grupo de clases de ideales del subcampo de grado p^γ , $\gamma \leq n$. Sea D_n el kernel de la norma: $0 \rightarrow D_n \rightarrow {}_\ell C_n \xrightarrow{N} {}_\ell C_{n-1} \rightarrow 0$ donde en general, si A es un subgrupo abeliano ponemos ${}_\ell A := \{x \in A \mid \ell x = 0\}$. Entonces $D_n \neq 0$ si y solamente si $C_n \neq C_{n-1}$ y en este caso $\dim_{\mathbb{F}_\ell} D_n \geq f$. \square*

$$p^n \left\{ \begin{array}{c} K_n \\ \vdots \\ K_\gamma \\ \vdots \\ K_0 \end{array} \right\} p^\gamma$$

Demostración. Por la Proposición 13.7.35 se tiene que N es suprayectiva y N es un isomorfismo en ${}_\ell C_n \rightarrow {}_\ell C_{n-1} \iff D_n = 0 \iff {}_\ell C_n = {}_\ell C_{n-1}$. Sea $G = \text{Gal}(K_n/K_0)$. Entonces D_n es un G -módulo. Sea $\rho: G \rightarrow \text{Aut}(D_n)$ la representación de G en D_n . Veamos que ρ es 1-1, esto es, que la representación es *fiel*. Si ρ no fuese 1-1, entonces ρ es trivial en el único subgrupo de orden p , a saber, en $S = \text{Gal}(K_n/K_{n-1})$. Se tiene

$$N_{n,n-1}D_n = \left\{ \sum_{g \in S} gd \mid d \in D_n \right\} = \left\{ \sum_{g \in S} d \mid d \in D_n \right\} = {}_p D_n = 0.$$

Por otro lado, $|D_n| = \ell^s$ con $\ell \neq p$ lo cual implica que $pD_n = D_n = 0$. Supongamos pues que $D_n \neq 0$. Sea $D := D_n \otimes_{\mathbb{F}_\ell} \tilde{\mathbb{F}}_\ell$ la extensión de escalares

donde $\tilde{\mathbb{F}}_\ell$ es una cerradura algebraica de \mathbb{F}_ℓ . Entonces D es un G -módulo con acción $g \circ (d \otimes x) := gd \otimes x$.

Además, $\dim_{\tilde{\mathbb{F}}_\ell} D_n = \dim_{\tilde{\mathbb{F}}_\ell} D$. Sea $D \cong \bigoplus_{i=1}^t D_i$ con cada D_i -módulo irreducible. Se tiene que D es un $\tilde{\mathbb{F}}_\ell[G]$ -módulo. Puesto que $p \neq \ell$, veremos que $\tilde{\mathbb{F}}_\ell[G]$ es *semisimple*, esto es, si M es un $\tilde{\mathbb{F}}_\ell[G]$ -módulo y $N < M$ submódulo de M , entonces necesariamente $M \cong N \oplus N'$ como $\tilde{\mathbb{F}}_\ell$ -módulos para algún N' .

En efecto, sea N' un $\tilde{\mathbb{F}}_\ell$ -espacio vectorial tal que como espacios vectoriales, $M \cong N \oplus N'$. Sea $\pi: M \rightarrow N$ la proyección lineal. En particular, $\pi(x) = x$ para $x \in N$. Sea $\varphi := \frac{1}{p^n} \text{Tr}_G(\pi)$, esto es,

$$\varphi(y) = \frac{1}{p^n} \sum_{g \in G} g \circ \pi(y).$$

Puesto que $\pi: M \rightarrow N$, se define la acción de g en $\text{Hom}(M, N)$ por $(g \circ \varphi)(z) := g\varphi(g^{-1}z)$. En particular $(g \circ \pi)(y) = g\pi(g^{-1}y)$.

Sea $\varphi: M \rightarrow N$ un $\tilde{\mathbb{F}}_\ell[G]$ homomorfismo. Sea $j: N \rightarrow M$ el encaje. Entonces

$$\begin{aligned} (\varphi \circ j)(y) &= \varphi(y) = \frac{1}{p^n} \sum_{g \in G} (g \circ \pi)(y) = \frac{1}{p^n} \sum_{g \in G} g\pi(g^{-1}y) \\ &\stackrel{\substack{\uparrow \\ g^{-1}y \in N}}{=} \frac{1}{p^n} \sum_{g \in G} gg^{-1}y = \frac{1}{p^n} \sum_{g \in G} y = y, \end{aligned}$$

es decir $\varphi \circ j = \text{Id}_N$ y por lo tanto la sucesión

$$0 \longrightarrow N \xrightarrow{j} M \longrightarrow M/N \longrightarrow 0$$

$\swarrow \varphi$

se escinde y $M \cong N \oplus M/N$ como G -módulos.

Ahora bien, como $\tilde{\mathbb{F}}_\ell$ es algebraicamente cerrado, $\dim_{\tilde{\mathbb{F}}_\ell} D_i = 1$ para todo i debido a que $\tilde{\mathbb{F}}_\ell$ es semisimple, conmutativo y por lo tanto es un producto directo de *anillos simples*. Cada anillo simple es un anillo de matrices sobre $\tilde{\mathbb{F}}_\ell$ y como es conmutativo esto sucede únicamente cuando es igual a $\tilde{\mathbb{F}}_\ell$.

Ahora, G es fiel en D_n por lo G es fiel en algún D_i pues de lo contrario no sería fiel en el único subgrupo de orden p . Así, G opera fielmente en algún D_i . Si $G = \langle \sigma \rangle$, $D_i \cong \tilde{\mathbb{F}}_\ell$ y entonces $\varphi: G \rightarrow \text{Aut}(D_i)$ es 1-1. Sea $\varphi(\sigma) = a$, entonces $\varphi(\sigma^2) = a^2, \dots, 1 = \varphi(1) = \varphi(\sigma^{p^n}) = a^{p^n}$ y $\varphi(\sigma^{p^{n-1}}) = a^{p^{n-1}} \neq 1$. Por lo tanto $a = \zeta = \zeta_{p^n}$ es una raíz p^n -ésima primitiva de 1. Más precisamente

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & \text{Aut}(D \otimes \tilde{\mathbb{F}}_\ell) = \text{Aut}(D) \\
 & \searrow \rho & \\
 & & \text{Aut}(D_n)
 \end{array}
 \quad
 \begin{array}{l}
 \varphi(\sigma)|_{D_i} : D_i \longrightarrow D_i \\
 x \longmapsto \zeta x
 \end{array}$$

Sea $\{v_1, \dots, v_s\}$ una base de D_n sobre \mathbb{F}_ℓ , $s = t$. Entonces $\{1 \otimes v_1, \dots, 1 \otimes v_s\}$ es una base de D sobre $\tilde{\mathbb{Z}}_\ell$. Sea $D_i = \langle \omega \rangle$ con $\omega = \sum_{i=1}^s \lambda_i \otimes v_i$, $\lambda_i \in \mathbb{F}_\ell$, $\sigma\omega = \zeta\omega = \sum_{i=1}^s \zeta\lambda_i \otimes v_i$.

Por otro lado, $\sigma\omega = \sum_{i=1}^s \lambda_i \otimes \sigma v_i$. Sea

$$\begin{array}{l}
 \rho: G \longrightarrow \text{Aut}(D_n) \\
 \sigma \longmapsto A = (a_{ij}) \quad (\text{matriz sobre } \mathbb{F}_\ell).
 \end{array}$$

Por tanto

$$\begin{aligned}
 \sigma\omega &= \sum_{i=1}^s \left\{ \lambda_i \otimes \left(\sum_{j=1}^s a_{ij} v_j \right) \right\} = \sum_{i=1}^s \sum_{j=1}^s \lambda_i a_{ij} \otimes v_j \\
 &= \sum_{k=1}^s \left(\sum_{j=1}^s \lambda_j a_{jk} \right) \otimes v_k,
 \end{aligned}$$

lo cual implica que $\zeta\lambda_k = \sum_{j=1}^s a_{jk} \lambda_j$.

Se sigue que $(A - \zeta I) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = 0$, esto es, ζ es raíz del polinomio característico $f(T) \in \mathbb{F}_\ell[T]$ de A . Ahora bien, $s = \text{gr } f(T)$ y $\text{gr } f(T) \geq \text{gr Irr}(T, \zeta, \mathbb{F}_\ell)$. Puesto que $f = [\mathbb{F}_\ell(\zeta) : \mathbb{F}_\ell]$ se sigue que $f \leq s$. \square

Corolario 13.7.55. Sea D una representación finito dimensional de un grupo cíclico G de orden p^n sobre \mathbb{F}_ℓ con $\ell \neq p$. Si D es fiel, entonces $\dim_{\mathbb{F}_\ell} D \geq f$ donde $f = o(\ell \text{ mód } p^n)$. \square

Teorema 13.7.56. Sea K_∞/K_0 una extensión \mathbb{Z}_p y sea C_n el ℓ -subgrupo de Sylow del grupo de clase $\text{Cl}(K_n)$ de K_n donde ℓ es un primo diferente a p . Si los ℓ -rangos de C_n están acotados, es decir, $\dim_{\mathbb{F}_\ell} \frac{C_n}{\ell C_n} \leq M$ para toda n y algún $M > 0$, entonces los órdenes de C_n están acotados.

Observación 13.7.57. El enunciado del Teorema 13.7.56 se puede pensar en algo así como si $\mu_\ell = 0$, entonces $\mu_\ell = \lambda_\ell = 0$.

Demostración (Teorema 13.7.56). En caso de que los órdenes no estuviesen acotados se tendría que $D_n \neq 0$ para n suficientemente grande. Puesto

$$f_n = o(\ell \text{ mód } p^n) \xrightarrow{n \rightarrow \infty} \infty \quad \text{se sigue que} \quad \dim_{\mathbb{F}_\ell} D_n \xrightarrow{n \rightarrow \infty} \infty$$

lo cual implica que $\dim_{\mathbb{F}_\ell} \ell C_n = \dim_{\mathbb{F}_\ell} \frac{C_n}{\ell C_n} \xrightarrow{n \rightarrow \infty} \infty$. \square

Observación 13.7.58. El Teorema 13.7.56 no es únicamente aplicable a las extensiones \mathbb{Z}_p . Por ejemplo, dado un campo numérico K y ℓ un número primo, o bien los ℓ -rangos de C_L tienen a infinito o $Cl(L)(\ell) = Cl(K)(\ell)$ cuando $p \rightarrow \infty$.

Teorema 13.7.59. Sea K_∞/K_0 una extensión \mathbb{Z}_p tal que K_n es campo de tipo MC. Sea ℓ un número primo distinto de p y supongamos que $\zeta_\ell \in K_0$. Si $|C_n^-(\ell)|$ está acotado, entonces $|C_n^+(\ell)|$ también está acotado.

Demostración. Por el Teorema 13.7.38 se tiene $\dim_{\mathbb{F}_\ell} \ell C_n^+ \leq \dim_{\mathbb{F}_\ell} \ell C_n^- + 1$ por lo tanto los ℓ -rangos de $C_n^+(\ell)$ están acotados. Por el Teorema 13.7.56, $|C_n^+(\ell)|$ están acotados. \square

13.8. Ejemplo de $\mu > 0$

En esta sección presentamos los ejemplos contruidos por Iwasawa de extensiones \mathbb{Z}_p donde $\mu > 0$.

Proposición 13.8.1 (Takagi y Chevalley). Sea L/K una extensión cíclica finita de campos numéricos con grupos de Galois G . Sea C_L el grupo de clases de ideales de L y sea $Cl_L^G := \{c \in Cl_L \mid c^g = c \ \forall g \in G\}$. Sean

$$e_0(L|K) := \prod_{\mathfrak{p} \in \mathbb{P}_K} e(\mathfrak{P}|\mathfrak{p}), \quad e_\infty(L|K) := \prod_{\substack{\mathfrak{p}_\infty, \text{ primos} \\ \text{infinitos}}} e(\mathfrak{P}_\infty|\mathfrak{p}_\infty)$$

y sean E_L y E_K los grupos de unidades de L y K respectivamente. Entonces

$$|Cl_L^G| = \frac{h(K)e(L|K)}{[L:K][E_K : N_{L/K} L^* \cap E_K]}$$

donde $h(K)$ es el número de clase de K y $e(L|K) = e_0(L|K)e_\infty(L|K)$.

Demostración. Sean P_L es grupo de ideales fraccionarios principales de L y I_L el grupo de ideales fraccionarios no cero de L . Se tiene la sucesión exacta $0 \rightarrow P_L \rightarrow I_L \rightarrow C_L \rightarrow 0$. En cohomología, obtenemos la sucesión exacta

$$0 \rightarrow P_L^G \rightarrow I_L^G \rightarrow Cl_L^G \rightarrow H^1(G, P_L) \rightarrow H^1(G, I_L) \rightarrow \dots$$

Ahora bien $H^1(G, I_L) = \frac{\text{núcl } N_G|_{I_L}}{I_G I_L}$. Se tiene que si $G = \langle \sigma \rangle$, $I_G I_L = \langle \sigma - 1 \rangle I_L$ y

$$H^1(G, I_L) = \frac{\langle \mathfrak{P}/\mathfrak{P}^\sigma \mid \mathfrak{P} \in \mathbb{P}_L \rangle}{\langle \mathfrak{P}/\mathfrak{P}^\sigma \mid \mathfrak{P} \in \mathbb{P}_L \rangle} = \{0\}.$$

Por tanto obtenemos la sucesión exacta

$$0 \longrightarrow P_L^G \longrightarrow \mathcal{C}l_L^G \longrightarrow H^1(G, P_L) \longrightarrow 0.$$

De donde

$$0 \longrightarrow I_L^G/P_L^G \longrightarrow \mathcal{C}l_L^G \longrightarrow H^1(G, P_L) \longrightarrow 0.$$

Se sigue que $|\mathcal{C}l_L^G| = [I_L^G : P_L^G] |H^1(G, P_L)|$.

Ahora bien, $I_L^G \supseteq P_L^G \supseteq P_K$ por lo que

$$[I_L^G : P_L^G] = \frac{[I_L^G : P_K]}{[P_L^G : P_K]} = \frac{[I_L^G : I_K][I_K : P_K]}{[P_L^G : P_K]}.$$

Por otro lado,

$$I_G^G = \langle \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \mid \mathfrak{p} \in \mathbb{P}_K \rangle, \quad I_K = \langle \mathfrak{p} \mid \mathfrak{p} \in \mathbb{P}_K \rangle = \langle (\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P})^{e(\mathfrak{P}|\mathfrak{p})} \mid \mathfrak{p} \in \mathbb{P}_K \rangle$$

lo cual implica que $[I_L^G : I_K] = e_0(L|K)$ y por ende $[I_L^G : P_L^G] = e_0(L|K) \frac{h_K}{[P_L^G : P_K]}$.

Ahora bien, se tiene la sucesión exacta

$$\begin{aligned} 1 \longrightarrow E_L \longrightarrow L^* \longrightarrow P_L \longrightarrow 0 \\ \alpha \longmapsto \langle \alpha \rangle \end{aligned}$$

con lo cual obtenemos en cohomología la sucesión exacta

$$0 \longrightarrow E_L^G = E_K \longrightarrow (L^*)^G = K^* \longrightarrow P_L^G \longrightarrow H^1(G, E_L) \longrightarrow H^1(G, L^*)$$

con $H^1(G, L^*) = \{0\}$ por Teorema 90 de Hilbert.

Se sigue que

$$0 \longrightarrow K^*/E_K \cong P_K \longrightarrow P_L^G \longrightarrow H^1(G, E_L) \longrightarrow 0$$

es exacta, lo cual implica que $[P_L^G : P_K] = |H^1(G, E_L)|$.

Para un G -módulo A se define la *cociente de Herbrand* por $\varphi(A) := \frac{h^0(A)}{h^1(A)} = \frac{|H^0(G, A)|}{|H^1(G, A)|}$. Se tiene que si A es finito, entonces $\varphi(A) = 1$ y si

$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta de G -módulos, entonces $\varphi(B) = \varphi(A)\varphi(C)$.

Se tiene que $\varphi(E_L) = \frac{e_\infty(L|K)}{[L:K]}$ y

$$\begin{aligned} \varphi(E_L)^{-1} |H^0(G, E_L)| &= |H^1(G, E_L)| = [P_L^G : P_K] \\ &= |H^0(G, E_L)| \cdot \frac{[L:K]}{e_\infty(L|K)}. \end{aligned}$$

Ahora bien, $H^0(G, E_L) = \frac{E_L^G}{N_{L/K} E_L} = \frac{E_K}{N_{L/K} E_L}$ por lo que $[P_L^G : P_K] = [E_K : N_{L/K} E_L] ([L:K] / e_\infty(L|K))$.

De la sucesión exacta $1 \longrightarrow E_L \longrightarrow L^* \longrightarrow P_L \longrightarrow 1$ se tiene la sucesión exacta

$$0 = H^1(G, K^*) \longrightarrow H^1(G, P_L) \longrightarrow H^0(G, E_L) \xrightarrow{\varphi} H^0(G, L^*)$$

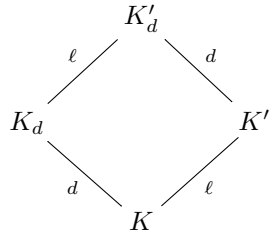
donde $\varphi: \frac{E_L^G}{N_{L/K} E_L} = \frac{E_K}{N_{L/K} E_L} \longrightarrow \frac{(L^*)^G}{N_{L/K} L^*} = \frac{K^*}{N_{L/K} L^*}$.

Se sigue que $H^1(G, P_L) \cong \text{nuc } \varphi = \frac{E_K \cap N_{L/K} L^*}{N_{L/K} E_L}$. Por tanto

$$\begin{aligned} |Cl_L^G| &= [I_L^G : I_K] |H^1(G, P_L)| = \frac{e_0(L|K) h_K}{[P_L^G : P_K]} |H^1(G, P_L)| \\ &= \frac{e_0(L|K) h_K}{\frac{|H^0(G, E_L)| [L:K]}{e_\infty(L|K)}} \cdot [E_K \cap N_{L/K} L^* : N_{L/K} E_L] \\ &= \frac{e(L|K) h_K}{[E_K : N_{L/K} E_L] [L:K]} \cdot [E_K \cap N_{L/K} L^* : N_{L/K} E_L] \\ &= \frac{e(L|K) h_K}{[L:K] [E_K : E_K \cap N_{L/K} L^*]}. \quad \square \end{aligned}$$

Lema 13.8.2. Sea ℓ un entero, $\ell \geq 2$. Sea K_d una extensión de un campo numérico K de grado d . Sean $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ ideales primos de K que se descomponen totalmente en K_d . Sea K' una extensión cíclica de K de grado ℓ en la cual $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ son totalmente ramificados. Sea $K'_d := K' K_d$. Entonces $\frac{|Cl_{K'_d}|}{|Cl_{K_d}|}$ es divisible por $\ell^{(t - [K:\mathbb{Q}])d-1}$.

Demostración.



Se tiene que K_d y K' son linealmente disjuntos pues los ideales primos \mathfrak{q}_i son totalmente ramificados en K' y totalmente descompuestos en K_d , $[K'_d : K_d] = \ell$. Aplicamos la Proposición de Takagi-Chevalley a la extensión cíclica K'_d/K_d y donde obtenemos, con $G = \text{Gal}(K'_d/K_d)$, que:

$$|\mathcal{Cl}_{K'_d}^G| = \frac{e(K'_d|K_d)|\mathcal{Cl}_{K_d}|}{[K'_d : K_d][E_{K_d} : E_{K_d} \cap N_{K'_d/K_d}(K'_d)^*]}.$$

Se tiene $E_{K_d}^\ell \subseteq E_{K_d} \cap N_{K'_d/K_d}(K'_d)^*$ lo cual implica que

$$\begin{aligned} \frac{|\mathcal{Cl}_{K'_d}|}{|\mathcal{Cl}_{K_d}|} &= \frac{|\mathcal{Cl}_{K'_d}|}{|\mathcal{Cl}_{K'_d}^G|} \frac{|\mathcal{Cl}_{K'_d}^G|}{|\mathcal{Cl}_{K_d}|} \\ &= \frac{e(K'_d|K_d)}{[K'_d : K_d][E_{K_d} : E_{K_d}^\ell]} \cdot [E_{K_d} \cap N_{K'_d/K_d} K'_d : E_{K_d}^\ell] \cdot \frac{|\mathcal{Cl}_{K'_d}|}{|\mathcal{Cl}_{K_d}^G|}. \end{aligned}$$

Se sigue que $\frac{e(K'_d|K_d)}{\ell \cdot [K'_d : K_d][E_{K_d} : E_{K_d}^\ell]} \Big| \frac{|\mathcal{Cl}_{K'_d}|}{|\mathcal{Cl}_{K_d}|}.$

Ahora bien, sobre cada \mathfrak{q}_i hay d primos en K_d y cada uno de ellos es totalmente ramificado en K'_d/K_d lo cual implica que $\ell^{td}|e(K'_d|K_d)$. Además tenemos $[K'_d : K_d] = \ell$.

Por el teorema de las unidades de Dirichlet, tenemos que si $s = r_1 + r_2 \leq r_1 + 2r_2 = [K_d : \mathbb{Q}] = d[K : \mathbb{Q}]$, entonces $E_{K_d} \cong \mathbb{Z}^{s-1} \times (\text{grupo finito})$.

Se tiene que $[E_{K_d} : E_{K_d}^\ell] = \ell^s$ o ℓ^{s-1} correspondiendo cada caso a si $W_{K_d}(\ell) \neq \{1\}$ o $W_{K_d}(\ell) = \{1\}$ respectivamente. Por lo tanto $[E_{K_d} : E_{K_d}^\ell]|\ell^{d[K:\mathbb{Q}]}$ lo cual implica que $\frac{e(K'_d|K_d)}{\ell \cdot [E_{K_d} : E_{K_d}^\ell]}$ es dividido por $\ell^{td-d[K:\mathbb{Q}]-1}$ y finalmente obtenemos que $\ell^{d(t-[K:\mathbb{Q}])-1} \Big| \frac{|\mathcal{Cl}_{K'_d}|}{|\mathcal{Cl}_{K_d}|}.$ \square

Todo lo anterior es la base en los ejemplos en que Iwasawa encontró extensiones \mathbb{Z}_p tales que $\mu > 0$.

Teorema 13.8.3. Sea $K_\infty/K_0 = K$ una extensión \mathbb{Z}_p . Sean $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ ideales primos de K que se descomponen totalmente en K_∞ . Sea K' una extensión cíclica de K de grado ℓ en donde $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ son totalmente ramificados. Entonces si $K'_\infty = K_\infty K'$ y $K'_n = K_n K'$, se tiene que si $\ell^{e'_n} = |\mathcal{Cl}_{K'_n}(\ell)|$ entonces $e'_n \geq (t - [K : \mathbb{Q}])p^n - 1$.

Demostración. Se tiene

$$\begin{array}{ccccc} K'_0 & - & - & - & K'_n & - & - & - & K'_\infty \\ | & & & & | & \ell & & & | \\ K_0 & - & - & - & K_n & - & - & - & K_\infty \end{array}$$

$[K'_n : K_n] = \ell$ y el resultado es consecuencia del Lema 13.8.2. \square

Para dar un ejemplo donde $\mu > 0$, necesitamos una extensión \mathbb{Z}_p donde exista una infinidad de primos totalmente descompuestos en K_∞/K . En

es caso, podemos tomar t arbitrariamente grande. Procedemos así: primero agregamos la raíz ζ_ℓ :

$$\begin{array}{ccc} K_0(\zeta_\ell) & \text{---} & K_\infty(\zeta_\ell) \\ | & & | \\ K_0 & \text{---} & K_\infty \end{array}$$

En ese caso se verifica que si hay una infinidad de primos totalmente descompuestos en $K_\infty(\zeta_\ell)/K_0(\zeta_\ell)$, entonces también hay una infinidad de primos totalmente descompuestos en K_∞/K_0 , esto es, podemos suponer que $\zeta_\ell \in K_0 = K$.

Sea $\alpha \in K$ tal que $v_{\mathfrak{q}_i}(\alpha) = 1$ para $1 \leq i \leq t$, es decir

$$\langle \alpha \rangle = \mathfrak{q}_1 \cdots \mathfrak{q}_t \mathfrak{a}$$

con \mathfrak{a} primo relativo a \mathfrak{q}_i , $1 \leq i \leq t$. Sea $K' := K_0(\alpha^{1/\ell})$.

Entonces $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ son ramificados en K' y por lo tanto $\mu_{K'} \geq t - [K : \mathbb{Q}] > 0$ cuando $\ell = p$ y $e'_n \geq (t - [K : \mathbb{Q}])p^n - 1$, $\ell^{e'_n}$ es la potencia de ℓ que divide a $h(K'_n)$.

Teorema 13.8.4. *Sea K un campo numérico finito de tipo MC. Entonces*

- (I) *Existe una extensión \mathbb{Z}_p , K_∞/K que es Galois sobre K^+ tal que si $\Gamma = \text{Gal}(K_\infty/K)$, entonces $\Gamma = \Gamma^-$.*

$$\begin{array}{ccc} K & \xrightarrow{\Gamma} & K_\infty \\ \{1, J\} \Big| & \nearrow G & \\ K^+ & & \end{array}$$

Se tiene la sucesión $1 \longrightarrow \Gamma \longrightarrow G \longrightarrow \{1, J\} \longrightarrow 1$ donde J actúa en Γ por conjugación.

- (II) *Sea \mathfrak{q}^+ un primo de K^+ que no divide a p y es inerte en K , y sea \mathfrak{q} el respectivo primo en K . Entonces \mathfrak{q} se descompone completamente en K_∞ y por el teorema de densidad de Cevotarev, hay una infinidad de tales primos \mathfrak{q}^+ y \mathfrak{q} . Por la observación anterior, existe K'/K tal que K'_∞/K_0 tiene invariante de Iwasawa $\mu' > 0$.*

Demostración. Sea M la máxima p -extensión abeliana de K no ramificada fuera de p . En particular $K_\infty \subseteq M$. Se tiene $\mathcal{G} := \text{Gal}(M/K) \sim U_p/\overline{E}$, donde $U_p := \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$ y \overline{E} es la cerradura de las unidades globales en U_p . Se tiene

$$\begin{array}{ccc} K & \xrightarrow{\mathcal{G}} & M \\ \{1, J\} \Big| & \searrow \mathfrak{E} & \\ K^+ & & \end{array} \quad 1 \longrightarrow \mathcal{G} \longrightarrow \mathfrak{E} \longrightarrow \{1, J\} \longrightarrow 1.$$

Cada primo “real” \mathfrak{p}^+ sobre p en K^+ permanece primo en K o se descompone en un producto de dos primos $\mathfrak{p}_1, \mathfrak{p}_2$ en K . En cada caso tenemos que

$\prod_{\mathfrak{p}|\mathfrak{p}^+} U_{\mathfrak{p}} \subseteq U_p$ y vía el mapeo exponencial obtenemos que hay un subgrupo de índice finito isomorfo a $\prod_{\mathfrak{p}|\mathfrak{p}^+} p^m \mathcal{O}_{\mathfrak{p}}$.

Sea $A := \prod_{\mathfrak{p}|p} p^m \mathcal{O}_{\mathfrak{p}}$. Se tiene la sucesión exacta

$$0 \longrightarrow A^- \longrightarrow A \xrightarrow{1+J} (1+J)A \longrightarrow 0$$

donde $A^- = \text{núc}(1+J)$ y $\text{rango}_{\mathbb{Z}_p} A^- = \text{rango } A/(1+J)A$. Se tiene que $A^{1+J} \subseteq p^m \mathcal{O}_{\mathfrak{p}^+}$, por tanto $\text{rango}_{\mathbb{Z}_p} A/(1+J)A \geq 1$ lo cual implica que $\text{rango}_{\mathbb{Z}_p} A^- \geq 1$. Por lo tanto $\text{rango}_{\mathbb{Z}_p} U_p^- \geq 1$.

Más aún, \overline{E} contiene un subgrupo de índice finito el cual está fijo bajo J ($[E : E^+] < \infty$) y por lo tanto \overline{E}^+ está fijo bajo conjugación compleja. Por simplicidad suponemos $p > 2$ y para $\mathcal{G} = \text{Gal}(M/K)$ tenemos que $\mathcal{G} \cong \mathcal{G}^+ \times \mathcal{G}^-$ y $\text{rango}_{\mathbb{Z}_p} \mathcal{G}^- \geq 1$. Por lo tanto existe un factor Γ de \mathcal{G} tal que $\Gamma = \Gamma^- \cong \mathbb{Z}_p$.

Se sigue que Γ es el grupo de Galois de una extensión \mathbb{Z}_p K_{∞} de K la cual es normal sobre K^+ pues si $\sigma : K_{\infty} \rightarrow \overline{\mathbb{Q}}$ es un encaje con $\sigma|_{K^+} = \text{Id}_{K^+}$ entonces $\sigma(K) = K$ y $\sigma|_K \in \text{Gal}(K/K^+) = \{1, J\}$. Se tiene $K_{\infty}^J = K_{\infty}$. Si $\sigma|_K = \text{Id}$, entonces $\sigma \in \Gamma$ por lo que $\sigma(K_{\infty}) = K_{\infty}$. Si $\sigma|_K = J$ entonces $J \circ \sigma = \text{Id}$ por lo que $J \circ \sigma(K_{\infty}) = K_{\infty}$ y $\sigma(K_{\infty}) = J(K_{\infty}) = K_{\infty}$.

Sea \mathfrak{q}^+ un primo de K^+ inerte en K/K^+ , con $\mathfrak{q}^+|p$. Sea D el grupo de descomposición de \mathfrak{q}^+ en $G = \text{Gal}(K_{\infty}/K^+)$. Entonces D es topológicamente cíclico pues \mathfrak{q} es no ramificado en K_{∞} . Ahora bien, se tiene que $G = \langle \gamma, J \mid J\gamma J = \gamma^{-1}, \gamma \in \Gamma \rangle$ ya que $\text{Gal}(K/K^+) = \langle 1, J \rangle \cong \{1, J\}$ y $J \circ \gamma = J\gamma J^{-1} = J\gamma J = \gamma^{-1}$. $K \xrightarrow{\Gamma} K_{\infty}, \quad \Gamma^- = \Gamma.$

$$\begin{array}{c} \{1, J\} \\ \left| \right. \\ K^+ \end{array}$$

Puesto que \mathfrak{q}^+ permanece primo en K , no se puede tener que $D \subseteq \Gamma$ lo cual implica que D contiene un elemento $J\gamma$ de orden 2 lo cual finalmente implica que \mathfrak{q} se descompone totalmente en K_{∞}/K . \square

Observación 13.8.5. Para $p = 2$ se toma el grupo factor G/G^{1+J} para obtener la menos parte y el argumento es esencialmente el mismo que en el caso p impar.

Veamos otros resultados.

Teorema 13.8.6 (L. Washington). Sea k una extensión abeliana de \mathbb{Q} y sea K/k la extensión \mathbb{Z}_p -ciclotómica de k . Sea $\ell \neq p$ un número primo y sea ℓ^{e_n} la potencia exacta de ℓ que divide al número de clase $h_n = h(K_n)$ de K_n . Entonces e_n está acotado y más precisamente, e_n es constante para n suficientemente grande. \square

Observación 13.8.7. El Teorema 13.8.6 no se cumple si la extensión K/k no es la ciclotómica (ver Teorema 13.8.3).

Teorema 13.8.8 (L. Washington). *Sea k un campo numérico abeliano imaginario, esto es, $\text{Gal}(k/\mathbb{Q})$ es un grupo abeliano y $K \not\subseteq \mathbb{R}$. Sea K/k la extensión \mathbb{Z}_p -ciclotómica de k . Sean*

$$h_n = h(K_n) \quad y \quad H = \{\ell \mid \ell \text{ es primo y } \ell \mid h_n^- \text{ para algún } n\}.$$

Entonces H es infinito. \square

Finalmente veamos los invariantes de Iwasawa en campos de funciones.

Sea k_0 un campo de funciones con campo de constantes el campo finito de q elementos \mathbb{F}_q , $q = \ell^m$ con ℓ un número primo. Sea $k_n := k_0 \cdot \mathbb{F}_{q^{p^n}}$. Entonces $\text{Gal}(k_n/k) \cong \text{Gal}(\mathbb{F}_{q^{p^n}}/\mathbb{F}_q) \cong \mathbb{Z}/p^n\mathbb{Z}$. Sea $k_\infty := \bigcup_{n=1}^{\infty} k_n$. Entonces $\text{Gal}(k_\infty/k_0) \cong \Gamma \cong \mathbb{Z}_p$.

Consideramos la *función zeta* de k_0 : $Z_{k_0}(u) = Z_0(u) = \frac{P_0(u)}{(1-u)(1-qu)}$ donde $P(u) \in \mathbb{Z}[u]$ es un polinomio de grado $2g$ y g es el género de k_0 . Se tiene que el número de clase de k_0 está dado por $h_0 = h(k_0) = P_0(1)$.

Sea $Z_{k_n}(v)$ la función zeta de k_n . Entonces

$$Z_{k_n}(v) = Z_{k_n}(u^{p^n}) = \prod_{j=1}^{p^n} Z_{k_0}(\zeta_{p^n}^j u).$$

Por otro lado tenemos que $P_0(u) = \prod_{i=1}^{2g} (1 - \alpha_i^{-1}u)$ donde $\alpha_1, \dots, \alpha_{2g}$ son las raíces de $P_0(u)$. Por lo tanto $P_n(u^{p^n}) = \prod_{i=1}^{2g} (1 - \alpha_i^{-p^n} u^{p^n})$ lo cual implica que

$$\begin{aligned} \frac{h_n}{h_0} &= \frac{P_n(1)}{P_0(1)} = \frac{\prod_{i=1}^{2g} (1 - \alpha_i^{-p^n})}{\prod_{i=1}^{2g} (1 - \alpha_i^{-1})} = \frac{\prod_{i=1}^{2g} \prod_{j=1}^{p^n} (1 - \zeta_{p^n}^j \alpha_i^{-1})}{\prod_{i=1}^{2g} (1 - \alpha_i^{-1})} \\ &= \prod_{i=1}^{2g} \prod_{j=1}^{p^n-1} (1 - \zeta_{p^n}^j \alpha_i^{-1}) =: A_n. \end{aligned}$$

Se sigue que $v_p(A_n) = \lambda n + \gamma$ para n suficientemente grande y $\lambda \leq 2g$. En particular $\mu = 0$. Es decir tenemos:

Teorema 13.8.9. *Para campos de funciones congruentes los invariantes de Iwasawa satisfacen que $\lambda \leq 2g$, donde g es el género del campo y $\mu = 0$. \square*

Referencias

1. Albert, A.A., *Cyclic fields of degree p^n over F of characteristic p* , Bulletin A.M.S. **40**, 625–631, (1934).
2. Albu, Toma *Cogalois theory*, Pure and Applied Mathematics a Dekker Series of Monographs and Textbooks, Inc, New York, 2003.
3. Artin, Emil & Schreier, Otto, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Hamburg Abhandlungen **5**, 225–231, (1926–1927).
4. Atiyah, Michael Francis & Macdonald, Ian G., *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
5. Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310, (1996).
6. Barrera–Mora, Fernando; Rzedowski–Calderón & Villa–Salvador, Gabriel, *On cogalois extensions*, J. Pure Appl. Algebra **76**, 1–11, (1991).
7. Barrera–Mora Fernando & Yslas–Velez, William, *Some results on radical extensions*, J. of Algebra **162**, 295–301, (1993).
8. Bautista–Ancona, Víctor, Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Genus Fields of Cyclic l -extensions of Rational Function Fields*, International Journal of Number Theory **9**, no. 5, 1249–1262, (2013).
9. Carlitz, Leonard, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1**, 137–168, (1935).
10. Carlitz, Leonard, *A class of polynomials*, Trans. Amer. Math. Soc. **43**, 137–168, (1938).
11. Chevalley, Claude, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys No. **6**, New York, American Mathematical Society XI, 1951.
12. Chi, Wen–Chen & Li, Anly *Kummer theory of division points over Drinfeld modules of rank one*, J. Pure Appl. Algebra **156**, no. 2–3, 171–185, (2001).
13. Clement, Rosario, *The genus field of an algebraic function field*, J. Number Theory **40**, no. 3, 359–375, (1992).
14. Deuring, Max, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Mathematics **314**, Berlin–Heidelberg–New York, Springer–Verlag, 1973.
15. Fine B., Rosenberg G., *Number Theory. An introduction via the Distribution of Primes*. Birkhäuser, 2007.

16. Fröhlich, Albrecht, *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics, **24**, American Mathematical Society, Providence, RI, 1983.
17. Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.
18. Greither, Cornelius and Harrison David Kent, *A Galois correspondece for radical extensions of fields*, J. Pure Appl. Algebra **43**, 257–270, (1986).
19. Hall, Marshal Jr. *Teoría de los grupos*, Editorial F. Trillas, México, 1969.
20. Hasse, Helmut, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper*, J. Reine Angew. Math. **172**, 37–54, (1934).
21. Hasse, Helmut, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3**, 45–51, (1951).
22. Hasse, Helmut *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie. Teil Ia: Beweis zu Teil I. Teil II: Reziprozitätsgesetz*, Würzburg–Wien: Physica–Verlag **135**, (1965).
23. Hasse, Helmut, *Eine Folgerung aus H.–W. Leopoldts Theorie der Geschlechter abelscher Zahlkörper*, Math. Nachr. **42**, 261–262, (1969).
24. Hasse, Helmut, *A supplement to Leopoldt's theory of genera in abelian number fields*, J. Number Theory **1**, 4–7, (1969).
25. Hayes, David R., *Explicit Class Field Theory for Rational Function Fields*, Trans. Amer. Math. Soc. **189**, 77–91, (1974).
26. Hilbert, David, *Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper*, Nachr. Ges. Wiss. zu Gottingen **1**, 29–39 (1896/97).
27. Hilbert, David, *The Theory of Algebraic Number Fields (Theorie der algebraischen Zahlkörper, Zahlbericht)*, Springer–Verlag, 1998.
28. Hilton, Peter & Wu, Yel Chiang, *Curso de álgebra moderna*, Editorial Reverté, Barcelona, 1982.
29. Hsu, Chih-Nung, *On Artin conjecture for the Carlitz module*, Compositio Mathematica **106**, 247–266, (1997).
30. Hu, Su & Li, Yan, *The genus fields of Artin–Schreier extensions*, Finite Fields Appl. **16**, no. 4, 255–264, (2010).
31. Ishida, Makoto, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, Vol. **555**, Springer–Verlag, Berlin–New York, 1976.
32. Iwasawa, Kenkichi, *On Γ -extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65**, 183–226, (1959).
33. Iwasawa, Kenkichi, *On the μ -invariants of cyclotomic fields*, Acta Arith. **21**, 99–101, (1972).
34. Iwasawa, Kenkichi, *On Z_l -extensions of algebraic number fields*, Ann. of Math. (2) **98**, 246–326, (1973).
35. Iwasawa, Kenkichi, *Riemann–Hurwitz formula and p -adic Galois representations for number fields*, Tôhoku Math. J. (2) **33**, no. 2, 263–288, (1981).
36. Iwasawa, Kenkichi, *Algebraic functions*, Translated from the 1973 Japanese edition by Goro Kato. Translations of Mathematical Monographs, **118**, American Mathematical Society, Providence, RI, 1993.
37. Iwasawa, Kenkichi, *Collected papers. Vol. I, II*, Edited and with a preface by Ichiro Satake, Genjiro Fujisaki, Kazuya Kato, Masato Kurihara and Shoichi Nakajima. With an appreciation of Iwasawa's work in algebraic number theory by John Coates, Springer–Verlag, Tokyo, 2001.

38. Januz, Gerald J., *Algebraic Number Fields*, Academic Press, New York, San Francisco, London, 1973.
39. Kronecker, Leopold, *Über die algebraisch auflöbaren Gleichungen (I. Abhandlung)*, Ber. K. Akad. Wiss. Berlin, 365–374 (Werke **4**, 1–11), (1853).
40. Lam–Estrada Pablo & Villa–Salvador, Gabriel, *Some remarks on the theory of cyclotomic function fields*, Rocky Mountain Journal of Mathematics **31**, no. 2, 483–502, (2001).
41. Landau, Edmund Georg Hermann, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig u. Berlin: B. G. Teubner. X (1909). Reimpresión AMS Chelsea Publishing, 2000.
42. Lang, Serge, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, Springer–Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1986.
43. Lang, Serge, *Cyclotomic fields I and II, Combined second edition, With an appendix by Karl Rubin*, Graduate Texts in Mathematics, **121**, Springer–Verlag, New York, 1990.
44. S. Lang. *Algebra 3rd ed.*, Addison–Wesley Co, Reading, Mass, 1993.
45. Leopoldt, Heinrich W., *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9**, 351–362, (1953).
46. Leopoldt, Heinrich–Wolfgang, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209**, 54–71, (1962).
47. Maldonado–Ramírez, Myriam R., Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Genus Fields of Abelian Extensions of Congruence Rational Function Fields*, Finite Fields and Their Applications **20**, 40–54 (2013).
48. Murty, M. Ram & Esmonde, Jody, *Problems in Algebraic Number Theory*, Second Edition, Graduate Texts in Mathematics **190**, Springer–Verlag, 2005.
49. Narkiewicz, Wladyslaw, *Elementary and Analytic Theory of Algebraic Numbers*, Second Edition, Springer–Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, 1990.
50. Neukirch, Jürgen, *Class field theory*, Springer–Verlag, Berlin, Heidelberg, New York, Tokyo, 1986.
51. Neukirch, Jürgen, *Algebraic number theory*, Springer–Verlag, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 1999.
52. Neumann, Olaf, *Two proofs of the Kronecker–Weber theorem “according to Kronecker, and Weber”*, J. Reine Angew. Math. **323**, 105–126 (1981).
53. Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98**, no. 2, 221–227, (2003).
54. Ribes, Luis & Zalesskii Pavel, *Profinite Groups*, Springer–Verlag, Ergebnisse der Mathematik und ihrer Ganzgebiete Folge 3, **40**, 2000.
55. Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378, (1987).
56. Rosen, Michael, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer–Verlag, New York, 2002.
57. Rzedowski Calderón, Martha & Villa Salvador, Gabriel D., *Conductor–Discriminant Formula for Global Function Fields*, International Journal of Algebra, **5**, no. 32, 1557–1565, (2011).
58. Salas Torres, Julio Cesar & Rzedowski Calderón, Martha, *Caracteres de Dirichlet en campos de funciones*, Soc. Mat. Mexicana, Aportaciones Mat. Comun., **36**, 127–144, (2006).

59. Salas Torres, Julio Cesar, Rzedowski Calderón, Martha & Villa Salvador, Gabriel, *Tamely ramified extensions and cyclotomic fields in characteristic p* , Palestine Journal of Mathematics **2** (1), 1–5, (2013).
60. Salas Torres, Julio Cesar, Rzedowski Calderón, Martha & Villa Salvador, Gabriel D., *Artin–Schreier and Cyclotomic Extensions*, JP Journal of Algebra, Number Theory and Applications **30**, No. 2, 173–190, (2013).
61. Salas Torres, Julio Cesar, Rzedowski Calderón, Martha & Villa Salvador, Gabriel, *A combinatorial proof of the Kronecker–Weber Theorem in positive characteristic*, Finite Fields and Their Applications **26**, 144–161, (2014).
62. Sánchez Mirafuentes, Marco & Villa Salvador, Gabriel, *Kummer Type Extensions in Function Fields*, International Journal of Algebra **7**, no. 4, 157–166, (2013).
63. Sánchez Mirafuentes, Marco & Villa Salvador, Gabriel, *Radical Extensions for the Carlitz Module*, Journal of Algebra **398**, 284–302, (2014).
64. Schmid, Hermann Ludwig, *Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p* , J. Reine Angew. Math. **175**, 108–123, (1936).
65. Schmid, Hermann Ludwig, *Zur Arithmetik der zyklischen p -Körper*, J. Reine Angew. Math. **176**, 161–167 (1937).
66. Schultheis, Fred, *Carlitz–Kummer Function Fields*, Journal of Number Theory **36**, 133–144, (1990).
67. Serre, Jean–Pierre *Local fields*, Graduate Texts in Mathematics **67**, New York–Hedelberg–Berlin, Springer–Verlag, 1979.
68. Stichtenoth, Henning, *Algebraic Function Fields and Codes*, Springer–Verlag, Universitext, Berlin–Heidelberg–New York, 1993.
69. Villa Salvador, Gabriel, *Introducción a la Teoría de las Funciones Algebraicas*, Fondo de Cultura Económica, México, 2003.
70. Villa Salvador, Gabriel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.
71. Villa Salvador, Gabriel, *An elementary proof of the conductor–discriminant formula*, Internatinal Journal of Number Theory, Vol. **6**, No. 5, 1191–1197, (2010).
72. Villa Salvador, Gabriel. *Analog of the Kronecker–Weber theorem in positive characteristic*, in Algebraic Curves and Finite Fields. Cryptography and Other Applications, Radon Series on Computational and Applied Mathematics **16**, Harald Niederreiter, Alina Ostafe, Daniel Panario, Arne Winterhof (Eds.), 213–237, De Gruyter 2014.
73. Washington, Lawrence C, *Class numbers and \mathbb{Z}_p -extensions*, Math. Ann. **214**, 177–193, (1975).
74. Washington, Lawrence C, *The non p -parts of the class numbers in a cyclotomic \mathbb{Z}_p -extensions*, Inventiones Math. **49**, 87–97, (1978).
75. Washington, Lawrence C, *Introduction to cyclotomic fields, Second edition*, Graduate Texts in Mathematics, **83**, Springer–Verlag, New York, 1997.
76. Weber, Heinrich Martin, *Theorie der Abelschen Zahlkörper*, Acta Math. **8**, 193–263, (1886).
77. Witt, Ernst, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f* , J. Reine Angew. Math. **174**, 237–245, (1936).

- 78. Witt, Ernst, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p* , J. Reine Angew. Math. **176**, 126–140, (1936).
- 79. Zhang, Xianke, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94**, no. 3, 393–395, (1985).